This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

+ *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.

+ *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.

+ *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.

+ *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at `http://books.google.com/`

Informazioni su questo libro

Si tratta della copia digitale di un libro che per generazioni è stato conservata negli scaffali di una biblioteca prima di essere digitalizzato da Google nell'ambito del progetto volto a rendere disponibili online i libri di tutto il mondo.

Ha sopravvissuto abbastanza per non essere più protetto dai diritti di copyright e diventare di pubblico dominio. Un libro di pubblico dominio è un libro che non è mai stato protetto dal copyright o i cui termini legali di copyright sono scaduti. La classificazione di un libro come di pubblico dominio può variare da paese a paese. I libri di pubblico dominio sono l'anello di congiunzione con il passato, rappresentano un patrimonio storico, culturale e di conoscenza spesso difficile da scoprire.

Commenti, note e altre annotazioni a margine presenti nel volume originale compariranno in questo file, come testimonianza del lungo viaggio percorso dal libro, dall'editore originale alla biblioteca, per giungere fino a te.

Linee guide per l'utilizzo

Google è orgoglioso di essere il partner delle biblioteche per digitalizzare i materiali di pubblico dominio e renderli universalmente disponibili. I libri di pubblico dominio appartengono al pubblico e noi ne siamo solamente i custodi. Tuttavia questo lavoro è oneroso, pertanto, per poter continuare ad offrire questo servizio abbiamo preso alcune iniziative per impedire l'utilizzo illecito da parte di soggetti commerciali, compresa l'imposizione di restrizioni sull'invio di query automatizzate.

Inoltre ti chiediamo di:

+ *Non fare un uso commerciale di questi file* Abbiamo concepito Google Ricerca Libri per l'uso da parte dei singoli utenti privati e ti chiediamo di utilizzare questi file per uso personale e non a fini commerciali.

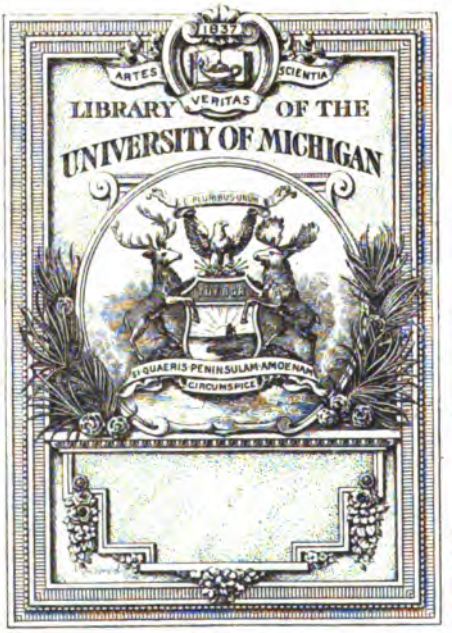
+ *Non inviare query automatizzate* Non inviare a Google query automatizzate di alcun tipo. Se stai effettuando delle ricerche nel campo della traduzione automatica, del riconoscimento ottico dei caratteri (OCR) o in altri campi dove necessiti di utilizzare grandi quantità di testo, ti invitiamo a contattarci. Incoraggiamo l'uso dei materiali di pubblico dominio per questi scopi e potremmo esserti di aiuto.

+ *Conserva la filigrana* La "filigrana" (watermark) di Google che compare in ciascun file è essenziale per informare gli utenti su questo progetto e aiutarli a trovare materiali aggiuntivi tramite Google Ricerca Libri. Non rimuoverla.

+ *Fanne un uso legale* Indipendentemente dall'utilizzo che ne farai, ricordati che è tua responsabilità accertati di farne un uso legale. Non dare per scontato che, poiché un libro è di pubblico dominio per gli utenti degli Stati Uniti, sia di pubblico dominio anche per gli utenti di altri paesi. I criteri che stabiliscono se un libro è protetto da copyright variano da Paese a Paese e non possiamo offrire indicazioni se un determinato uso del libro è consentito. Non dare per scontato che poiché un libro compare in Google Ricerca Libri ciò significhi che può essere utilizzato in qualsiasi modo e in qualsiasi Paese del mondo. Le sanzioni per le violazioni del copyright possono essere molto severe.

Informazioni su Google Ricerca Libri

La missione di Google è organizzare le informazioni a livello mondiale e renderle universalmente accessibili e fruibili. Google Ricerca Libri aiuta i lettori a scoprire i libri di tutto il mondo e consente ad autori ed editori di raggiungere un pubblico più ampio. Puoi effettuare una ricerca sul Web nell'intero testo di questo libro da `http://books.google.com`


1837
ARTES
VERITAS
SCIENTIA
LIBRARY OF THE
UNIVERSITY OF MICHIGAN
E PLURIBUS UNUM
SI QUAERIS PENINSULAM AMOENAM
CIRCUMSPICE

QA
171
.B57

TEORIA

DEI

69807

GRUPPI DI SOSTITUZIONI

E DELLE

EQUAZIONI ALGEBRICHE

SECONDO GALOIS

LEZIONI FATTE

nella R. Scuola Normale Superiore di Pisa l'anno accademico 1896-97

DAL

Prof. LUIGI BIANCHI

RACCOLTE E PUBBLICATE PER CURA

DEL

Dott. VITTORIO BOCCARA

PISA

R. LITOGRAFIA FF. GOZANI

—

1897

Parte prima

Teoria dei gruppi di sostituzioni

§1. — **Sostituzioni e loro composizione.** — Consideriamo n oggetti che contrassegniamo con n lettere

$$x_1 \; x_2 \; x_3 \ldots\ldots\ldots\ldots x_n$$

e tutte le $1.2.3\ldots\ldots n. = \pi(n)$ permutazioni che si possono fare su questi oggetti, cangiandone l'ordine. — L'operazione per la quale si passa da una permutazione degli n oggetti ad un'altra dicesi una **sostituzione**; essa si indica simbolicamente, scrivendo fra parentesi la permutazione da cui si parte ed al disopra la permutazione che deve sostituirla. — Diciamo subito che si riguardano come identiche due sostituzioni, quando a ciascuna lettera (oggetto) sostituiamo la medesima lettera; così per es. le due sostituzioni

$$\begin{pmatrix} x_3 & x_4 & x_1 & x_5 & x_2 \\ x_1 & x_2 & x_3 & x_4 & x_5 \end{pmatrix} \qquad \begin{pmatrix} x_1 & x_4 & x_3 & x_2 & x_5 \\ x_3 & x_2 & x_1 & x_5 & x_4 \end{pmatrix}$$

sono identiche. Se si indicano quindi con

$$\sum_1 \sum_2 \sum_3 \qquad\qquad \sum_{\pi(n)}$$

le $\pi(n!)$ permutazioni, essendo per es. $\sum_1$ la permutazione $x_1 \dots x_n$, avremo evidentemente le $\pi(n!)$ sostituzioni distinte

$$\begin{pmatrix} \sum_1 \\ \sum_1 \end{pmatrix} \begin{pmatrix} \sum_2 \\ \sum_! \end{pmatrix} \dots\dots\dots\dots\dots \begin{pmatrix} \sum_{\pi(n)} \\ \sum_1 \end{pmatrix}.$$

Fra queste la prima, che lascia ogni lettera al suo posto, dicesi **la sostituzione identica** o **l'identità**. Spesso si rappresentano le sostituzioni con lettere $S, T \dots\dots$ ed in particolare l'identità col simbolo 1.

Essendo S, T due qualunque sostituzioni possiamo considerare la sostituzione U che nasce eseguendo prima S, poi T; essa dicesi la sostituzione composta delle due od anche il loro prodotto e si indica simbolicamente con

$$U = ST$$

ponendo a sinistra la sostituzione eseguita prima. (*)

(*) Alcuni adottano la notazione inversa TS; ciò è naturalmente indifferente, ma poichè diremo nel testo è necessario fissare la convenzione fondamentale a riguardo di equivoci.

Osserviamo subito che non è in generale

$$ST = TS$$

così p. es. se si prende

$$S = \begin{pmatrix} x_3 & x_4 & x_2 & x_1 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix} \qquad T = \begin{pmatrix} x_4 & x_3 & x_2 & x_1 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}$$

abbiamo

$$ST = \begin{pmatrix} x_2 & x_1 & x_3 & x_4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}, \quad TS = \begin{pmatrix} x_1 & x_2 & x_4 & x_3 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}$$

Quando le due sostituzioni S, T soddisfano alla condizione $ST = TS$ si dicono fra loro **permutabili**.—

Invece di comporre due sole sostituzioni fra loro possiamo comporne un numero qualunque

$$S_1, S_2, \ldots\ldots S_m$$

e per prodotto

$$S_1 S_2 \ldots\ldots S_m$$

intendiamo la sostituzione che risulta eseguendo prima S_1, poi S_2, indi S_3 ecc, in fine S_m.— (*)

Mentre per un prodotto di sostituzioni non vale, in generale, la legge **commutativa**, vale però, come per un ordinario prodotto, la legge **associativa**.— Per un prodotto di tre sostituzioni si verifica subito la detta proprietà,

---

(*) Propriamente dovremmo indicare il prodotto così:

$$\big(\ldots\ldots\big((S_1 S_2)\cdot S_3\big)\ldots\ldots\big)S_m$$

espressa simbolicamente dalla formula

$$(S_1 S_2) \cdot S_3 = S_1 \cdot (S_2 S_1)$$

poichè se x_i è una lettera qualunque che da S_1 sia portata in x_k, mentre S_2 porti x_k in x_l e la S_3 x_l in x_m, si vede che ambedue le sostituzioni composte portano x_i in x_m. — È chiaro ora che valendo la legge associativa pel prodotto di tre sostituzioni, vale in generale.

Osserviamo poi che se le tre sostituzioni S, T coincidono ed U è una sostituzione qualunque, coincideranno altresì i due prodotti SU, TU, come pure gli altri due US, UT, onde si vede che:

I due membri di una eguaglianza $S = T$ di due sostituzioni possono moltiplicarsi dalla medesima parte (a destra o a sinistra) per una medesima sostituzione.

§2. — Periodo di una sostituzione. —

Quando gli m fattori del prodotto

$$S_1 S_2 \ldots\ldots S_m$$

sono eguali fra loro e ad una medesima sostituzione S, il prodotto stesso dicesi la m^{ma} potenza di S, e si indica con S^m. — A causa della legge associativa è

chiaro che due potenze di una stessa sostituzione si moltiplicano fra loro sommando gli esponenti, cioè:

$$(1) \qquad S^m \cdot S^p = S^{m+p} \qquad (*)$$

Si definiscono altresì le potenze con esponente negativo introducendo la sostituzione **inversa** di S, quella cioè che composta con S dà luogo all'identità; questa sostituzione inversa si indica col simbolo S^{-1} e se simbolicamente

$$S = \begin{pmatrix} \Sigma_i \\ \Sigma_o \end{pmatrix}$$

$$S^{-1} = \begin{pmatrix} \Sigma_o \\ \Sigma_i \end{pmatrix}$$

Poichè $S\,S^{-1} = 1$, per naturale estensione della formula (1) intenderemo che sia

$$S^0 = 1$$

Ciò posto essendo m un numero intero positivo definiremo S^{-m} come la potenza m^{ma} di S^{-1}:

$$S^{-m} = (S^{-1})^m,$$

dopo di che la (1) varrà evidentemente qualunque siano gli esponenti interi m, p positivi o negativi.-

---

(*) Ne segue che le potenze di una medesima sostituzione sono sostituzioni permutabili.-

Ora formiamo la serie delle successive potenze di S:

(2) $\quad S^0 = 1\,,\ S\,,\ S^2,\ S^3 \ldots\ldots\ldots\ldots$

Il numero delle sostituzioni possibili essendo finito ed uguale a $\pi(n)$, da un certo punto in poi nella serie (2) le sostituzioni si ripeteranno. La prima a ripetersi sarà certamente l'identità poichè da

$$S^{\alpha+\beta} = S^{\alpha}$$

moltiplicando per $S^{-\alpha}$ segue $S^{\beta} = 1$.

Il più piccolo esponente β positivo pel quale

$$S^{\beta} = 1$$

dicesi il periodo della sostituzione S.

Allora le β potenze di S

(3) $\qquad 1\,,\ S\,,\ S^2,\ \ldots\ldots\ldots\ S^{\beta-1}$

sono tutte distinte ma ogni altra potenza S^{α} comunque α negativo o positivo è eguale ad una delle (3).

È infatti se z indica il minimo resto positivo di $\alpha \pmod{\beta}$ sarà

$$\alpha = q\beta + z \qquad (q \text{ intero})$$

quindi

$$S^{\alpha} = (S^{\beta})^q \cdot S^z = S^z$$

Di qui si trova subito: Due potenze S^p, S^q di S sono <u>eguali</u> allora ed allora soltanto che gli esponenti p, q siano congrui fra loro rispetto al

periodo β di S.—

Essendo β il periodo di S, è facile determinare il periodo β_1 di qualsiasi potenza S^α di S.— Vediamo infatti che: Se δ è il massimo comun divisore di α e di β sarà $\beta_1 = \frac{\beta}{\delta}$ il periodo di S^α.— In particolare nella serie (3) vi sono $\varphi(\beta)$ potenze col periodo β cioè tante quanti sono i numeri della serie $1, 2, 3, \ldots\ldots \beta-1$ primi con β.—

§3.— Sostituzioni circolari.—

Una sostituzione S dicesi circolare o ciclica quando le lettere da esse spostate possono ordinarsi in guisa che la S porti ciascuna lettera in quella che la segue e l'ultima nella prima. così p. es. $S = \begin{pmatrix} x_3 & x_1 & x_4 & x_2 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}$ opera ciclicamente sulla permutazione $(x_2\, x_1\, x_3\, x_4)$ e però è ciclica.— Una sostituzione ciclica si scrive più brevemente racchiudendo fra parentesi la permutazione sulla quale opera ciclicamente; così nell'esempio superiore scriviamo

$$S = (x_2\, x_1\, x_4\, x_4)$$

È chiaro che se n sono le lettere sulla quale S opera ciclicamente si può così scrivere in n modi diversi. Il periodo di una sostituzione ciclica su n lettere è evidentemente eguale

le ad n. – Dimostriamo ora che: Qualunque sostituzione S può scindersi nel prodotto di più sostituzioni cicliche. * Prendiamo infatti una lettera qualunque x_i, e sia x_{i_2} quella che la sostituisce, così x_{i_3} quella che sostituisce x_{i_2} ecc ecc. Nella successione di lettere

$$x_i, x_{i_2}, x_{i_3}, \ldots\ldots$$

la prima a ripetersi, come subito si vede (*), è la x_{i_1} e se supponiamo che per tale operazione si ottengano le r lettere diverse

$$x_i, x_{i_2}, \ldots\ldots, x_{i_{r-1}}$$

sopra di queste la S opererà precisamente come la sostituzione ciclica

$$(x_i, x_{i_2}, \ldots\ldots, x_{i_{r-1}})$$

Presa ora una altra lettera x_{k_1} oltre la precedente, si formi nello stesso modo il ciclo relativo e così via. – La S rimarrà così decomposta appunto nel prodotto di tante sostituzioni circolari $S = C_1 C_2 C_3 \ldots\ldots C_\sigma$ (1)
e si noti che queste sostituzioni circolari, operando ciascuna su lettere diverse, sono due a due permutabili. –

(*) Se fosse invece la x_{i_s} $(s>1)$ ripetuta dalla $x_{i_{s+1}}$ la $x_{i_{s-1}}$, che va in x_{i_s}, dovrebbe già essere identica alla x_{i_2} che va in $x_{i_{s+1}} = x_{i_s}$

La rappresentazione (4) di una sostituzione S come prodotto di sostituzioni circolari è quella che torna più spesso utile. — Vediamo intanto che da essa può subito riconoscersi quale è il periodo della S poichè:

Il periodo di una sostituzione S è dato dal minimo multiplo comune degli ordini (periodi) dei suoi cicli. — Ed infatti se β è il periodo di S dev'essere

$$C_1^\beta C_2^\beta \ldots\ldots C_s^\beta = 1$$

e poichè ciascun ciclo C opera su lettere diverse, dovremo avere separatamente

$$C_1^\beta = 1 \quad , \quad C_2^\beta = 1 \; ; \ldots\ldots\ldots\ldots C_s^\beta = 1$$

onde β dovrà essere multiplo dei singoli periodi di C_1, $C_2 \ldots C_s$; inversa per ogni multiplo β di tutti questi periodi è $S^\beta = 1$

§4. — **Trasposizioni. — Sostituzioni pari e sostituzioni dispari.** — Dicesi trasposizione una sostituzione ciclica su due lettere. — Ora diciamo che:

Qualunque sostituzione può scindersi nel prodotto di più trasposizioni. — Per dimostrarlo basta osservare che con una trasposizione si può

portare una lettera al posto che deve effettivamente occupare: resta allora da fare una sostituzione in cui manca questa lettera e che può quindi trattarsi nel medesimo modo. Una sostituzione si può decomporre in modi diversi nel prodotto di trasposizioni (*), ma in qualunque modo si decomponga, il numero delle trasposizioni nel prodotto sarà sempre pari o sempre dispari. Per dimostrarlo osserviamo che se S è una sostituzione decomposta in cicli, ove espressamente osserviamo che valutiamo anche come cicli quelli composti di una sola lettera: moltiplicando S a destra (o a sinistra) per una trasposizione U, il numero dei cicli crescerà ovvero diminuirà di una unità. Ed invero se U opera sopra due lettere di un medesimo ciclo C in S, possiamo evidentemente supporre che una di esse sia la prima del ciclo C, poniamo

$$C = (x_1\, x_2 \cdots x_{i-1}\, x_i\, x_{i+1} \cdots x_m)$$

$$U = (x_1\, x_i)$$

allora abbiamo

$$C\,U = (x_1\, x_2 \cdots x_{i-1})(x_i\, x_{i+1} \cdots x_m)$$

(*) Es. $(x_1\, x_2\, x_3\, x_4\, x_5) = (x_1\, x_2)(x_1\, x_3)(x_1\, x_4)(x_1\, x_5)$

$= (x_1\, x_4)(x_2\, x_4)(x_4\, x_5)(x_3\, x_5)(x_1\, x_5)(x_1\, x_4)$

ed al ciclo C di S ne troviamo sostituiti due in SU.(*) Se le lettere su cui opera U appartengono a due cicli diversi C, C', poniamo

$$C = (x_1\, x_2 \ldots\ldots x_z)$$
$$C' = (y_1\, y_2 \ldots\ldots y_s)$$
$$U = (x_1\, y_1)$$

onde

$$CC'U = (x_1\, x_2 \ldots\ldots x_z\, y_1\, y_2 \ldots\ldots y_s)$$

e i due cicli C, C' di S si riuniscono in SU in uno solo, ciò che dimostra l'asserzione.—

Ora supponiamo che scelte n lettere

$$x_1\, x_2 \ldots\ldots\ldots x_n$$

si abbia una sostituzione S composta di k cicli (**) e sia decomposta nel prodotto di m trasposizioni

$$S = U_1\, U_2 \ldots\ldots\ldots U_m\ ;$$

avremo dunque

$$S U_m U_{m-1} \ldots\ldots\ldots U_2\, U_1 = 1$$

e poichè l'identità è una sostituzione con n cicli e

(*) N. B. Se $z = 2$ ovvero $z = m$ uno di due cicli consta di una sola lettera.—

(**) Cf. l'avvertenza superiore.—

ad ogni moltiplicazione per una ν il numero dei cicli cresce o diminuisce di 1, sarà

$$k + m \equiv n \pmod 2$$

$$m \equiv n + k \pmod 2$$

Se quindi la S si decompone in un altro prodotto di m' trasposizioni si avrà

$$m' \equiv m \pmod 2 \qquad \text{c.d.d.}$$

Questi teoremi danno luogo a distinguere le sostituzioni in due classi secondo che constano di un numero pari o di un numero dispari di trasposizioni; le prime diconsi sostituzioni **pari**, le seconde **dispari**. È chiaro che un prodotto di più sostituzioni è pari o dispari secondo che le sostituzioni componenti dispari sono in numero pari o dispari.

Ora se osserviamo che una sostituzione ciclica d'ordine r $\qquad (x_1\, x_2 \ldots\ldots\ldots x_r)$

equivale al prodotto di $r-1$ trasposizioni

$$(x_1 x_2)(x_1 x_3) \ldots\ldots\ldots (x_1 x_r)$$

vediamo che essa è pari o dispari secondo che r è dispari o pari. In generale una sostituzione che si decomponga in k cicli contenenti rispettivamente

$$n_1 \quad n_2 \ldots\ldots\ldots\ldots n_k$$

lettere equivale a

$$q = n_1 + n_2 + \cdots\cdots + n_k - k \qquad (*)$$

trasposizioni ed appartiene quindi alla prima o alla seconda classe secondo che $q \equiv 0$ ovvero $q \equiv 1 \pmod 2$

§5. Sostituzioni simili — Sostituzioni permutabili.

Se S, T sono due qualunque sostituzioni la sostituzione

$$U = T^{-1} S T$$

dicesi la trasformata di S per mezzo della T. (**) Supponiamo S decomposta in cicli e sia

$$C = (x_1\, x_2 \ldots\ldots x_r)$$

un suo ciclo; indichiamo poi con $y_1, y_2 \ldots\ldots y_r$ le lettere in cui T trasporta $x_1\, x_2 \ldots x_r$ rispettivamente. Poichè la T^{-1} trasporta y_i in x_i mentre la S trasporta x_i in x_{i+1} ed in fine la T trasporta x_{i+1} in y_{i+1} avremo manifestamente che

---

(*) In tale computo è evidentemente indifferente comprendere o no i cicli di una sola lettera.

(**) Inversamente si ha $S = T U T^{-1}$ onde S è trasformata di U per mezzo della T^{-1}

$$C' = (y_1\ y_2 \cdots y_2)$$

sarà un ciclo di $\tau^{-1}S\tau$. Dunque:

La trasformata $\tau^{-1}S\tau$ di S per mezzo di τ si ottiene da S effettuando sopra i suoi cicli la sostituzione τ.

È chiaro che S e $\tau^{-1}S\tau$ hanno lo stesso numero di cicli e nei cicli corrispondenti egual numero di lettere. Viceversa se due sostituzioni S, U soddisfano a queste condizioni, nel qual caso diconsi **simili**, sarà U una trasformata di S:

$$U = \tau^{-1}S\tau$$

Basta infatti prendere per τ una sostituzione che porti ogni lettera di un ciclo di S nella corrispondente del corrispondente ciclo in U. Notiamo ora le seguenti proposizioni:

1ª) Essendo S, τ due qualunque sostituzioni le due sostituzioni $S\tau$, τS sono simili. È invero.

$$S\tau = \tau^{-1}(\tau S)\tau$$

2ª) La trasformata di un prodotto è eguale al prodotto delle trasformate dei fattori. Infatti per la legge associativa:

$$(\mathcal{T}^{-1}S_1\mathcal{T})(\mathcal{T}^{-1}S_2\mathcal{T})\cdots\cdots(\mathcal{T}^{-1}S_r\mathcal{T}) = \mathcal{T}^{-1}(S_1S_2\cdots S_r)\mathcal{T}$$

In particolare
$$(\mathcal{T}^{-1}S\mathcal{T})^m = \mathcal{T}^{-1}S^m\mathcal{T}$$

§6. — **Gruppi di sostituzioni.** — Arriviamo ora all' importante e fondamentale concetto di gruppo di sostituzioni. — Un sistema di un numero qualsiasi di sostituzioni sopra n lettere dicesi un gruppo se il prodotto di due sostituzioni qualunque (differenti od eguali) nel sistema appartiene al sistema stesso. — In particolare si osservi che se un gruppo contiene una sostituzione S conterrà qualsiasi potenza di S e però anche l' identità. — Il concetto di gruppo sorto da prima appunto dalla teoria delle sostituzioni ha acquistato poi nelle matematiche un' estensione ed una importanza sempre maggiori perchè le teorie che ne derivano conservano la loro validità per tutte quelle serie discrete (finite o infinite) di operazioni per le quali esiste una legge di composizione e vale la legge associativa.

(*) Come esempio citiamo le sostituzioni lineari omogenee sopra n variabili che sono appunto operazioni suscettibili di composizione.

In seguito dimostreremo poi che lo studio di un gruppo finito qualsiasi di operazioni si riduce a quello di un gruppo di sostituzioni sopra lettere sicchè occupandoci, come ora faremo, di questi gruppi speciali noi studiamo altresì la teoria generale dei gruppi. —

Chiamasi **ordine** di un gruppo il numero delle sostituzioni (operazioni) che vi sono contenute. Il più semplice esempio di un gruppo si ottiene formando le potenze di una medesima sostituzione S; se β è il periodo di S, le β sostituzioni

$$1,\ S,\ S^2, \ldots\ldots S^{\beta-1}.$$

formano appunto un gruppo d'ordine β.

Un altro esempio di gruppo l'abbiamo nella totalità delle $\pi(n)$ sostituzioni sopra n lettere; questo dicesi **il gruppo totale**. È manifesto poi che fra le $\pi(n)$ sostituzioni del gruppo totale, quelle pari formano per sè un gruppo, il cui ordine è $\frac{\pi(n)}{2}$ (*); questo dicesi il **gruppo alterno**.

Dicesi <u>sottogruppo</u> di un gruppo G ogni gruppo le cui sostituzioni appartengono tutte a G; così p. es. ogni gruppo G contiene

(*) E infatti basta osservare che moltiplicando tutte le $\pi(n)$ sostituzioni per una trasposizione le pari si cangiano in dispari e viceversa [illegible] concludere che tante sono le une quante le altre. —

come sottogruppo il gruppo formato dalle potenze di una sostituzione qualunque S.

§7. Teorema fondamentale: L'ordine di un sottogruppo Γ di un gruppo G è sempre un divisore dell'ordine del gruppo.

Sia n l'ordine del gruppo G e p l'ordine del sottogruppo Γ; indicando con

$$S_1 = 1 , S_2 , \ldots\ldots S_p$$

le p sostituzioni di Γ scriviamo simbolicamente

$$(1) \qquad \Gamma = (S_1 S_2 \cdots S_p)$$

Sia ora t_2 una sostituzione di G non appartenente a Γ; se formiamo le p sostituzioni che risultano dal moltiplicare quelle di Γ p. es. a destra per t_2:

$$(2) \qquad S_1 t_2 , S_2 t_2 \cdots\cdots S_p t_2$$

è facile vedere che esse sono diverse fra loro e dalle precedenti. E invero da

$$S_i t_2 = S_k t_2$$

seguirebbe $S_i = S_k$ mentre da

$$S_i t_2 = S_k$$

verrebbe

$$t_2 = S_i^{-1} S_k = S_l$$

contro l'ipotesi che t_2 non appartenga a I. Ora tutte le sostituzioni (2) appartengono certamente a G, per la definizione stessa di gruppo; esse insieme colle (1) possono esaurire o no il gruppo G. Nel primo caso si ha evidentemente

$$m = 2p$$

e il teorema è verificato; nel secondo caso sia t_3 una sostituzione di G che non appartenga nè alla serie (1) (gruppo) nè alla (2). Se formiamo le p sostituzioni di G

$$(3) \qquad S_1 t_3 , S_2 t_3 , \ldots\ldots S_p t_3$$

vediamo subito ragionando nel medesimo modo, che esse sono tutte diverse fra loro e dalle $2p$ precedenti. Se le (1) (2) (3) insieme esaurissero G, sarà $m = 3p$, altrimenti si continuerà nel medesimo modo. E poichè le sostituzioni di G sono in numero finito m perverremo evidentemente a distribuire tutte le m sostituzioni di G in un quadro contenente un certo numero, diciamo r, di orizzontali ciascuna delle quali contiene p sostituzioni, cioè nel quadro

$$(A) \qquad \begin{array}{|llll|} \hline S_1 & S_2 & \ldots\ldots & S_p \\ S_1 t_2 & S_2 t_2 & \ldots\ldots & S_p t_2 \\ \ldots & \ldots & \ldots\ldots & \ldots \\ S_1 t_2 & S_2 t_2 & \ldots\ldots & S_p t_2 \\ \hline \end{array}$$

Si avrà allora $m = zp$ il che dimostra il teorema. — Il quoziente $z = \frac{m}{p}$ che si ottiene dividendo l'ordine m del gruppo G per l'ordine p del sottogruppo Γ dicesi l'**indice** del sottogruppo nel gruppo.

Al quadro (A) dovremo spesso ricorrere nel seguito; qualche volta lo scriveremo più brevemente sotto la forma

$$G = (\Gamma, \Gamma t_2, \Gamma t_3, \ldots \Gamma t_z)$$

È manifesto che invece di formare il nostro quadro moltiplicando a destra le sostituzioni di Γ per le nuove sostituzioni di G, si potrebbe invece moltiplicare a sinistra. Indicando allora con $\tau_2, \tau_3, \ldots \tau_z$ le sostituzioni moltiplicatrici, avremmo il quadro

(B)

S_1	S_2	. . . . .	S_p
$\tau_2 S_1$	$\tau_2 S_2$	. . . . .	$\tau_2 S_p$
$\tau_3 S_1$	$\tau_3 S_2$	. . . . .	$\tau_3 S_p$
. . . . .			
. . . . .			
$\tau_z S_1$	$\tau_z S_2$	. . . . .	$\tau_z S_p$

ovvero

$$G = (\Gamma, \tau_2\Gamma, \tau_3\Gamma, \ldots \tau_z\Gamma)$$

Il teorema fondamentale ora dimostrato ammette varii corollari dei quali qui rileviamo i più importanti:

1°) L'ordine di un gruppo di sostituzioni sopra n lettere è un divisore di $\pi(n)$.—

2°) Il periodo di qualsiasi sostituzione S di un gruppo G è un divisore dell'ordine di G.—

Notiamo ancora le proposizioni seguenti che derivano subito dalla definizione stessa di gruppo:

1°) Le sostituzioni comuni a due gruppi formano un nuovo gruppo, che è adunque sottogruppo di ambedue.

2°) Le sostituzioni di un gruppo G sopra lettere che non spostano certe lettere a, b, c..... formano un sottogruppo di G.

Ed infatti se due sostituzioni di G non spostano a, b, c... nemmeno il loro prodotto le sposta.—

3°) Le sostituzioni di un gruppo G permutabili con una medesima sostituzione T. (che può appartenere o no a G) formano in G un sottogruppo.—

Per vederlo basta osservare che, se S_1, S_2 sono due sostituzioni permutabili con T, anche il loro prodotto è permutabile con T. Ed invero si ha:

$$T^{-1} S_1 T = S_1 \qquad T^{-1} S_2 T = S_2$$

onde $$T^{-1}(S_1 S_2) = S_1 S_2$$

§8.- **Gruppo alterno**.- Come abbiamo visto, il gruppo totale $\mathcal{G}_{\pi(n)}$ sopra n lettere ammette come sottogruppo il gruppo alterno con $\frac{\pi(n)}{2}$ sostituzioni cioè coll'indice 2.- Ora sussiste il teorema: *Nel gruppo totale $\mathcal{G}$ sopra n lettere non esiste alcun altro sottogruppo d'indice 2 all'infuori del gruppo alterno.*-

Sia infatti

$$\Gamma = (S_1 \; S_2 \; \ldots\ldots \; S_{\frac{1}{2}\pi(n)})$$

un sottogruppo d'indice 2 in $\mathcal{G}$.- Indicando con T una qualunque sostituzione di $\mathcal{G}$ fuori di Γ e formando il quadro del §7, avremo

$$(\alpha) \qquad \mathcal{G} = \begin{cases} S_1 \; S_2 \ldots\ldots\ldots S_{\frac{1}{2}\pi(n)} \\ S_1 T, S_2 T \ldots\ldots\ldots S_{\frac{1}{2}\pi(n)} T \end{cases}$$

Ora se formiamo le sostituzioni

$$(\beta) \qquad S_1 T^2, \; S_2 T^2 \ldots\ldots\ldots\ldots$$

queste si troveranno certo comprese nel quadro (α), ma non nella 2ª orizzontale perchè da

$$S_i T^2 = S_i T$$

dedurremo $T = S_i^{-1} S_k$ cioè T apparterrebbe a $\mathfrak{T}$. Dunque la (β) saranno le S stesse in altro ordine; in generale, come tutto si vede una sostituzione

$$S_i T^z$$

apparterrà alla 1ª . 2ª orizzontale del quadro (α) secondo che l'esponente z di T è pari o dispari. Ne segue che il periodo di T è necessariamente pari e però tutte le sostituzioni di periodo dispari debbono trovarsi in T. Ciò vale in particolare delle sostituzioni circolari su tre lettere. — Il teorema enunciato sarà quindi dimostrato se proviamo che sussiste l'altro per sè stesso importante:

Se un gruppo sopra n lettere contiene tutte le sostituzioni circolari su tre lettere, esso coincide col gruppo alterno o col gruppo totale. —

Per dimostrare quest'ultimo teorema osserviamo che un prodotto di due trasposizioni può sempre compiersi con sostituzioni cicliche del 3º ordine, come si vede dalle identità

$$(a\,b)(c\,d) = (b\,c\,d)(a\,b\,c)$$

$$(a\,b)(b\,c) = (a\,c\,b)$$

Lo stesso accade dunque di qualunque sostituzione pari che si ottiene componendo prodotti di due trasposizioni. Un gruppo che contenga tutte le sostituzioni cicliche di 3° ordine contiene perciò tutte le sostituzioni pari cioè il gruppo alterno, il che dimostra il teorema.

Il teorema superiore può anche generalizzarsi dicendo che:

Se un gruppo contiene tutte le sostituzioni circolari sopra r lettere $(r \geq 2)$, esso coincide col gruppo alterno o col totale.

Infatti, se $r=2$ il gruppo contiene tutte le trasposizioni e perciò qualunque altra sostituzione; se $r=3$ siamo nel caso precedente. Il caso $r>3$ si riconduce a questo, osservando che una sostituzione ciclica su 3 lettere può comporsi con due sostituzioni circolari su $r>3$ lettere; infatti si ha:

$$(x_1 x_2 x_3) = (x_1 x_2 x_3 x_4 \ldots\ldots x_r)(x_1 x_2 x_3 x_4 \ldots\ldots x_r)^{-1}$$

§9. Gruppi transitivi ed intransitivi.

Rispetto ai gruppi di sostituzioni sopra n lettere ha grande importanza la distinzione dei gruppi in due classi e cioè in **gruppi transitivi** e **gruppi intransitivi**.

Sia G sopra n lettere $x_1 x_2 \ldots\ldots x_n$

si **transitivo** quando prese ad arbitrio due lettere x_i, x_k esiste sempre in G una sostituzione almeno che porta x_i in x_k; nel caso opposto dicesi **intransitivo**. Perchè un gruppo sia transitivo basta che si possa portare, con sostituzioni del gruppo, una lettera fissa p. es. x_1 in una arbitraria x_i. Sia infatti S una tale sostituzione e S' una sostituzione di G che porti x_1 in x_k; la sostituzione $S^{-1}S'$ porterà x_i in x_k. Se un gruppo G è intransitivo e la lettera a_1 può portarsi, con sostituzioni di G, al posto di $a_2, a_3, \ldots, a_q$ ma non al posto di alcuna lettera rimanente b, non esisterà in G alcuna sostituzione che porti una delle a per es. a_i in b. È invero se S è una sostituzione che porta a_1 in a_i e S' una sostituzione che porta a_1 in b, la SS' porterà a_1 in b contro l'ipotesi. Invece se prendiamo due qualunque delle a siano a_i a_k esisterà evidentemente in G una sostituzione che porta a_i in a_k. Sul gruppo di lettere

$$a_1 \; a_2 \; \ldots\ldots \; a_q$$

le sostituzioni di G operano quindi transitivamente. Diremo invece rispetto ad un gruppo intransitivo G, le lettere sulle quali opera G si scindono in sistemi in guisa che le sostituzioni di G operano transitivamente sulle lettere

di ciascun sistema ma non portano mai una lettera di un sistema in un'altro di sistema diverso.

Esempio. Se a, b, c, d sono quattro lettere e formiamo tutti i possibili prodotti di due trasposizioni, cioè

$$(a\,b)(c\,d)\,,\ (a\,c)(b\,d)\,,\ (a\,d)(b\,c)$$

questi, insieme all'identità, formano un gruppo d'ordine 4, che è transitivo.—

Se rispetto ad un gruppo intransitivo le lettere si dividono in sistemi di transitività

$$A_1\ A_2\ A_3\ \ldots\ldots\ldots$$

contenenti rispettivamente

$$n_1\ n_2\ n_3\ \ldots\ldots$$

lettere, essendo $n_1 + n_2 + n_3 + \ldots\ldots = n$ è facile vedere che:

L'ordine m di G sarà un divisore del prodotto $\pi(n_1)\pi(n_2)\pi(n_3)\ldots\ldots$

E infatti se formiamo il gruppo totale G_1 sulle n_1 lettere di A_1, il gruppo totale G_2 sulle n_2 lettere di A_2 ecc e formiamo tutti i possibili prodotti di una sostituzione di G_1 per una di G_2, di G_3 ecc otteniamo un gruppo d'ordine $\pi(n_1)\pi(n_2)\pi(n_3)\ldots\ldots$ che contiene G come sottogruppo.—

Nei gruppi transitivi si distingue poi il grado di transitività

dicendo che: Un gruppo G è m volte transitivo quando prese m lettere qualunque fra quelle su cui opera il gruppo ed altre m lettere pure ad arbitrio esistono in G sostituzioni che portano le prime ordinatamente nelle seconde. — (*)

Come per la semplice transitività si dimostrerà anche qui che un gruppo è m volte transitivo appena si possono portare, con sostituzioni del gruppo, m lettere fisse in m qualunque.

Un esempio di gruppi a transitività multipla l'abbiamo nel gruppo alterno su n lettere che è $n-2$ volte transitivo perchè se

$$x_{i_1}\ x_{i_2} \ldots\ldots\ldots\ x_{i_n}$$

è una qualunque permutazione delle n lettere, delle due sostituzioni

$$\begin{pmatrix} x_{i_1} & x_{i_2} & \ldots & x_{i_{n-2}} & x_{i_{n-1}} & x_{i_n} \\ x_1 & x_2 & & x_{n-2} & x_{n-1} & x_n \end{pmatrix}, \quad \begin{pmatrix} x_{i_1} & x_{i_2} & \ldots & x_{i_{n-2}} & x_{i_n} & x_{i_{n-1}} \\ x_1 & x_2 & & x_{n-2} & x_{n-1} & x_n \end{pmatrix}$$

(*) Naturalmente dicendo che G è m volte transitivo, intendiamo che non lo sia $m+1$ volte che cioè non si possano portare in $m+1$ lettere qualunque in altre $m+1$ qualunque.

una è pari e porta le $n-2$ prime lettere in $n-2$ arbitrarie. Il gruppo totale potrebbe riguardarsi, secondo la definizione, come n volte transitivo; però riguardo ai teoremi generali converrà considerarlo come $n-1$ volte transitivo. (*)

§10.- Teoremi sui gruppi transitivi.

Pei gruppi transitivi sussiste il teorema fondamentale: **L'ordine di un gruppo G m volte transitivo su n lettere è dato da**

$$k \cdot n(n-1)\ldots\ldots(n-m+1),$$

ove k è l'ordine di quel sottogruppo I di G che lascia ferme m lettere fissate ad arbitrio.

Rispetto al sottogruppo

$$I = S_1 S_2 \ldots\ldots S_k$$

che lascia ferme le m lettere $x_1, x_2 \ldots x_m$, distribuiamo le sostituzioni di G nel solito quadro (A) §4:-

$$G = \begin{cases} S_1 \; S_2 \ldots\ldots S_k \\ S_1 t_2, S_2 t_2 \ldots\ldots S_k t_2 \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ S_1 t_2 \; S_2 t_2 \ldots\ldots S_k t_2 \end{cases}$$

(*) Del resto è chiaro che un gruppo $n-1$ volte transitivo è necessariamente il gruppo totale.

dove con q abbiamo indicato l'indice di T in G. Si vedrà subito che due sostituzioni appartenenti alla stessa classe laterale nel gruppo portano $x_1, x_2 \ldots\ldots x_m$ nei medesimi posti, mentre due di classe laterale diversa le portano in posti differenti. — Ora essendo G m volte transitivo le m lettere $x_1 \ldots x_m$ vengono ad occupare per sostituzioni di G

$$n(n-1)\ldots\ldots(n-m+1)$$

posti diversi, onde appunto

$$q = n(n-1)\ldots\ldots(n-m+1).$$

Vediamo in particolare che il gruppo alterno ha il minimo ordine compatibile col suo grado di transitività.

Dimostriamo ora l'altro teorema: ..

In un gruppo m volte transitivo, che non coincida col gruppo alterno o col gruppo totale, nessuna sostituzione (eccetto l'identità) può spostare m lettere soltanto o meno di m lettere.

Naturalmente supponiamo $m \geq 2$, chè per $m=1$ la cosa è evidente per qualunque gruppo. Sia S una sostituzione di G che sposti al massimo m lettere, e T una sostituzione di G che porti queste lettere in altre affatto arbitrarie (come ne esiste certamente a causa della transitività

multipla di $\mathcal{G}$); la TST che è una qualunque delle sostituzioni simili a S appartiene dunque a $\mathcal{G}$.

Ciò posto decomponiamo S in cicli e sia

$$(x_1\, x_2\, x_3 \ldots\ldots x_p)$$

un suo ciclo e supponiamo dapprima che questo ciclo contenga almeno tre lettere e però che sia $m \geq 3$. Prendiamo la sostituzione S' simile ad S che abbia per un ciclo

$$(x_1\, x_3\, x_2\, x_4 \ldots\ldots x_p)$$

e gli altri identici a quelli di S; poiché la S', come si è detto, appartiene a $\mathcal{G}$ vi apparterrà anche

$$S' S^{-1} = (x_1\, x_2\, x_3)$$

Il gruppo $\mathcal{G}$ contenendo una e quindi tutte le sostituzioni circolari su tre lettere sarebbe quindi il gruppo alterno o il gruppo totale.

Se poi i cicli di S fossero tutti del 2° ordine, in numero di due o più, il che suppone $m \geq 4$, avremmo

$$S = (a_1 a_2)(a_3 a_4)(a_5 a_6) \cdots\cdots$$

ed anche la sostituzione simile

$$S_1 = (a_1 a_3)(a_2 a_4)(a_5 a_6) \ldots\ldots$$

sarebbe in $\mathcal{G}$ e però anche

$$\mathcal{U} = S S_1 = (a_1 a_4)(a_2 a_3) .$$

Ma essendo $m \geq 4$ quindi $n \geq 5$ vi sarebbe almeno una 5ª

lettera a_5 e $\mathfrak{G}$ conterrebbe anche

$$V = (a_1 a_5)(a_2 a_3)$$

e però

$$(\mathfrak{U} V) = (a_1 a_4 a_5)$$

cioè una sostituzione circolare su tre lettere, come sopra. In fine se $\mathfrak{I}$ fosse una trasposizione, $\mathfrak{G}$ conterrebbe tutte le trasposizioni e coincederebbe quindi col gruppo totale.

§11 — Limite del grado di transitività. — Dimostriamo ora un altro teorema il quale ci servirà, insieme ai precedenti, a fissare un limite superiore pel grado di transitività di un gruppo.

Premettiamo anzi tutto il seguente lemma:

Se un gruppo $\mathfrak{G}$ d'ordine $\underline{m}$ contiene due sottogruppi Γ, Γ' dei rispettivi ordini $\underline{n}, \underline{n'}$ e nessuna sostituzione di Γ (l'identità esclusa) è simile ad una sostituzione di Γ' sarà $\underline{m}$ multiplo del prodotto $n \cdot n'$. —

Supponiamo

$$\Gamma = (\gamma_1, \gamma_2 \cdots \gamma_n)$$

$$\Gamma' = (\gamma'_1, \gamma'_2 \cdots \gamma'_{n'})$$

e formiamo le nn' sostituzioni

$$\gamma_i^{\delta} \gamma'_i \quad \Big| \quad \delta = 1, 2, \ldots, n$$

Queste sono tutte distinte fra loro perchè da

$$\gamma_i \gamma'_k = \gamma_j \gamma'_\lambda$$

seguirebbe

$$\gamma_j^{-1} \gamma_i = \gamma'_\lambda \gamma'^{-1}_k$$

e quindi per l'ipotesi fatta

$$\gamma_j^{-1} \gamma_i = 1 \qquad \gamma'_\lambda \gamma'^{-1}_k = 1$$

cioè

$$\gamma_i = \gamma_j \quad , \quad \gamma'_k = \gamma'_\lambda$$

Se le 1) esaurissero le sostituzioni di $\mathfrak{G}$, si ha $m = m'$ ed il teorema è provato. In caso contrario prendasi in $\mathfrak{G}$ una sostituzione g fuori delle 1) e si formino le m' sostituzioni

$$2) \qquad \gamma_i g \gamma'_k \quad \begin{cases} i = 1, 2, \dots m \\ k = 1, 2, \dots m' \end{cases}$$

Queste sono differenti dalle 1) e fra di loro. È infatti se una delle 2) appartenesse alle 1) ne verrebbe che g stessa apparterrebbe alle 1); fra di loro poi perchè da

$$\gamma_i g \gamma'_k = \gamma_j g \gamma'_\lambda$$

seguirebbe

$$g^{-1} (\gamma_j^{-1} \gamma_i) g = \gamma'_\lambda \gamma'^{-1}_k$$

Ora $\gamma_j^{-1} \gamma_i$ è una sostituzione di $\mathfrak{I}$ che sarebbe dunque simile alla $\gamma'_\lambda \gamma'^{-1}_k$ di $\mathfrak{I}'$ e però come sopra

$$\gamma_i = \gamma_j \quad , \quad \gamma'_k = \gamma'_\lambda \, ,$$

basti [illegible] nel medesimo [illegible]

stiare il teorema fondamentale (§ 7) per riconoscere la verità della nostra asserzione.

Ciò posto, possiamo dimostrare:

«L'ordine k di un gruppo G m volte transitivo su n lettere, che non coincida col gruppo alterno o totale, è un divisore di

$$\frac{\pi(n)}{\pi(m)} = (m+1)(m+2)\dots n .»$$

È invero pel teorema alla fine del § precedente G non contiene alcuna sostituzione simile ad una sostituzione del gruppo totale T d'ordine $\pi(m)$ sopra m delle n lettere e però, pel lemma superiore, $k\,\pi(m)$ è un divisore di $\pi(n)$ c. d. d.

Ed ora possiamo fissare un limite superiore del grado di transitività di un gruppo col teorema:

Un gruppo di sostituzioni sopra n lettere, che non coincida col gruppo totale o alterno, non può essere più di $\left[\frac{n}{2}\right]$ (*) volte transitivo.

È infatti se k è l'ordine del gruppo, esso è un divisore di $\frac{\pi(n)}{\pi(m)}$ e multiplo di $n(n-1)\dots(n-m+1)$

(*) Per convenzione $\left[\frac{n}{2}\right]$ indica il massimo intero contenuto in $\frac{n}{2}$.—

onde

$$\frac{\pi(n)}{\pi(m)\,n(n-1)\ldots(n-m+1)} = \frac{\pi(n-m)}{\pi(m)}$$

è intero; dunque $n-m \geq m$, cioè $m \leq \frac{n}{2}$ c. a. d. Questo limite $\left[\frac{n}{2}\right]$ potrebbe essere molto abbassato con ulteriori teoremi, ma qui ci basta di avere rilevato come il gruppo totale e l'alterno si distinguano già dagli altri gruppi pel loro grado più alto di transitività.—

§12.—Gruppi imprimitivi e primitivi.— Un gruppo transitivo G dicesi imprimitivo quando le n lettere sulle quali opera possono distribuirsi in sistemi contenenti tutti un egual numero di lettere, in guisa che le sostituzioni di G lascino ciascuna lettera di un sistema nel proprio sistema ovvero portino tutte le lettere di un sistema contemporaneamente in quelle di un altro sistema.— Così p.e. rispetto al gruppo ciclico formato dalle potenze della sostituzione circolare su 6 lettere

$$(x_1\ x_2\ x_3\ x_4\ x_5\ x_6)$$

i due sistemi di lettere

$$x_1\ x_3\ x_5 \qquad\qquad x_2\ x_4\ x_6$$

appunto sistemi d' imprimitività.— Ma si osservi subito che un gruppo può essere in più modi imprimitivo, cioè può darsi che la divisione in sistemi d' imprimitività possa farsi in più modi. Così nel caso precedente i tre sistemi

$$x_1 x_4 \qquad x_2 x_5 \qquad x_3 x_6$$

formano ancora sistemi d' imprimitività. In generale si osserva che un gruppo dotato di transitività multipla non può mai essere imprimitivo perchè se a, b fossero due lettere di un sistema e c quella di un altro esisterebbe in G una sostituzione che porta a in b e b in c.— Un gruppo pel quale la divisione in sistemi di imprimitività è impossibile dicesi **primitivo**; dunque: **Ogni gruppo più volte transitivo è primitivo.**—

Supponiamo che G sia un gruppo imprimitivo; quelle sostituzioni di G che lasciano fermo ogni singolo sistema d' imprimitività formano evidentemente un sottogruppo T, che può del resto anche ridursi alla sola identità. Sia q l' indice di T in G e distribuiamo le sostituzioni di G nel solito quadro.

$$\mathfrak{G} = \begin{cases} \Gamma \\ \Gamma t_2 \\ \Gamma t_3 \\ \cdots \\ \cdots \\ \Gamma t_q \end{cases}$$

si vede subito che le sostituzioni appartenenti ad una medesima orizzontale e queste soltanto producono sui sistemi di imprimitività la stessa permutazione. E se consideriamo questi sistemi come altrettanti elementi (lettere)

$$A, B, C \ldots .$$

le q sostituzioni corrispondenti sopra $A, B, C \ldots$ formeranno un gruppo, sicchè se z è il numero di questi sistemi sarà q un divisore di $\pi(z)$.—

§13.— Dimostriamo il seguente teorema che ci sarà utile più tardi:

Se un gruppo transitivo $\mathfrak{G}$ sopra n lettere contiene una trasposizione, esso è imprimitivo, ovvero coincide col gruppo totale.

Il gruppo transitivo $\mathfrak{G}$ sopra n lettere

$$x_1, x_2 \ldots . x_n$$

contenga la trasposizione $(x_1 x_2)$. Se esso contenesse anche

tutte le trasposizioni

$$(x_1\, x_3)\ ,\ (x_1\, x_4)\ \ldots\ (x_1\, x_n)$$

conterrebbe qualsiasi trasposizione

$$(x_i\, x_k) = (x_1 x_i)(x_1 x_k)(x_1 x_i)$$

e però sarebbe il gruppo totale. Siano dunque

$$(x_1\, x_2)\ ,\ (x_1\, x_3), \ldots\ldots (x_1\, x_2) \qquad z < n$$

tutte le trasposizioni di G in cui figura x_1. Per quanto ora si è detto G conterrà tutte le possibili trasposizioni sulle z lettere

$$(\alpha) \qquad x_1\ x_2\ x_3 \ldots\ldots x_z$$

e però anche il gruppo totale su queste z lettere.
Ma è facile vedere che non conterrà alcuna altra trasposizione in cui figuri una lettera del sistema (α) poichè se p. es. contenesse la trasposizione

$$(x_i\, x_{z+1}) \qquad i \leq z$$

conterrebbe anche

$$(x_1 x_i)(x_i x_{z+1})(x_1 x_i) = (x_1\, x_{z+1})$$

contro l'ipotesi. Il gruppo G essendo transitivo se prendiamo un'altra lettera qualunque x_{i_1}, oltre le z lettere (α), esisteranno in G trasposizioni contenenti x_{i_1} e partendo da x_{i_1} come prima da x_1 possiamo formare il nuovo sistema di lettere (β) $\quad x_{i_1}\, x_{i_2}\, x_{i_3} \ldots\ldots x_{i_z}$ tale

che in G vi sono tutte le trasposizioni fra queste lettere ma nessun' altra trasposizione che contenga una soltanto di esse. Ora dimostriamo che tutte le lettere del sistema (β) sono, come la prima x_{i_1}, diverse da quelle del sistema (α) e il numero delle lettere nei due sistemi $(\alpha)(\beta)$ è eguale $(\tau = \tau)$. In G esiste certo (a causa della transitività) una sostituzione S che porta x_1 in x_{i_1}, quindi $x_2 x_3 \dots x_\tau$ in lettere del sistema (β) poichè se supponiamo per es.

$$S = \begin{pmatrix} x_{i_1} & x_{i_2} & \cdots \\ x_1 & x_2 & \cdots \end{pmatrix}$$

la trasposizione

$$S^{-1}(x_1 x_2) S = (x_{i_1}, x_{i_2})$$

congiunge x_{i_2} con x_{i_1}, e quindi x_{i_2} appartiene a (β).- D'altronde se fosse p. es. $x_{i_2} = x_2$ avremmo in G la trasposizione

$$(x_{i_1}, x_{i_2}) = (x_{i_1}, x_2)$$

cioè x_{i_1} apparterrebbe ad (α) contro l'ipotesi.- Adunque anche il sistema (β) contiene τ lettere

$$(\beta) \qquad x_{i_1}, x_{i_2} \dots \dots x_{i_\tau}$$

e se una sostituzione di G porta una lettera di (α) in una lettera di (β) trasporterà ad un tempo tutte le lettere di (α) in tutte quelle di (β). Così proseguendo

distribuiamo manifestamente le s lettere in un certo numero di sistemi contenenti ciascuno r lettere e questi sistemi saranno appunto sistemi di imprimitività c.d.d.

Dal teorema dimostrato risulta come corollario:

Se un gruppo transitivo sopra un numero primo di lettere contiene una trasposizione, coincide col gruppo totale.-

§ 14.- **Gruppi isomorfi**.- Le proprietà che abbiamo studiate negli ultimi paragrafi si riferiscono strettamente ai gruppi di sostituzioni sopra lettere; quelle che andiamo ora a trattare hanno un maggior grado di estensione applicandosi ai gruppi di operazioni qualunque (§ 6)

Supponiamo di avere dapprima due gruppi G, T del medesimo ordine e tali che ad ogni sostituzione g di G possa farsi corrispondere una sostituzione f di T per tal modo che al prodotto di due sostituzioni in G corrisponda sempre il prodotto (nel medesimo ordine) delle due corrispondenti in f; allora i due gruppi diconsi *isomorfi*.-

Naturalmente due sostituzioni corrispondenti g, f hanno

il medesimo periodo, onde segue che all' identità in $\mathfrak{G}$ corrisponde l' identità in T ed alla g^j la j^{ma}. Inoltre è chiaro che ad ogni sottogruppo di $\mathfrak{G}$ corrisponde in T un sottogruppo del medesimo ordine. — Come esempio di isomorfismo fra due gruppi si consideri una sostituzione ciclica S sopra n lettere e le sue potenze che costituiscono un gruppo $\mathfrak{G}$ d' ordine n. — Consideriamo poi attorno ad un asse fisso nello spazio una rotazione di $\frac{2\pi}{n}$; le potenze di questa rotazione formano un gruppo T isomorfo con $\mathfrak{G}$. — Possiamo generalizzare la nozione d' isomorfismo nel modo seguente. — Supponiamo che i due gruppi $\mathfrak{G}$, T non siano più del medesimo ordine ma ad ogni sostituzione g di T corrispondano più sostituzioni in $\mathfrak{G}$ e ad una di $\mathfrak{G}$ una sola in T sempre in guisa che al prodotto di due g corrisponda il prodotto delle due corrispondenti in T. Si dice allora che i due gruppi sono **meriedricamente isomorfi**, mentre nel caso prima considerato, della biunivocità della corrispondenza, l' isomorfismo di

---

(*) Se β è il periodo di g a $g^\beta = 1$ corrisponde γ^β e a $g^{\beta+1} = g$ corrisponde $\gamma^{\beta+1}$, onde $\gamma^{\beta+1} = \gamma$ cioè $\gamma^\beta = 1$ ecc. —

cesi oloedrico. Come esempio di isomorfismo meriedrico si consideri una sostituzione (operazione) S di periodo composto $m = pq$ e una sostituzione U di periodo p; i due gruppi

$$\mathfrak{G} = (1, S, S^2 \ldots S^{m-1})$$
$$T = (1, U, U^2 \ldots U^{p-1})$$

sono posti in relazione di isomorfismo meriedrico se ad ogni potenza S^k di $\mathfrak{G}$ si fa corrispondere quella potenza U^r di U che ha per esponente il minimo resto positivo di $k \pmod p$.

Supponiamo i due gruppi $\mathfrak{G}, T$ meriedricamente isomorfi e all'identità in $\mathfrak{G}$ corrispondano in T le n sostituzioni

$$\sigma_1 = 1, \sigma_2, \ldots \ldots \sigma_n$$

fra le quali naturalmente deve trovarsi l'identità. Le sostituzioni σ formano un gruppo Σ perchè a $\sigma_i \sigma_k$ in $\mathfrak{G}$ corrisponde in T la sostituzione $1 \cdot 1 = 1$. Distribuiamo ora le sostituzioni di $\mathfrak{G}$, rispetto al sottogruppo Σ, nel solito quadro

$$\mathfrak{G} = \begin{cases} \Sigma \\ \Sigma t_1 \\ \cdots \\ \Sigma t_q \end{cases}$$

essendo q l'indice di Σ in G cioè $m = nq$ l'ordine di G. Si vede subito che a due sostituzioni di G corrisponde la medesima sostituzione in T o sostituzioni diverse secondo che esse appartengono o no alla medesima orizzontale nel quadro. Abbiamo dunque il teorema:

Se i gruppi G, T sono meriedricamente isomorfi e alla identità in T corrispondono in G le n sostituzioni

$$\sigma_1 \quad \sigma_2 \ldots\ldots \sigma_n$$

queste formano in G un sottogruppo e ad ogni sostituzione in T corrispondono precisamente n sostituzioni in G. Il numero n dicesi il grado di meriedria.

§15. I gruppi generali di operazioni. Se due gruppi G, T sono oloedricamente isomorfi e, prescindendo dal significato particolare che possono avere le loro operazioni, si ha riguardo soltanto al modo come queste operazioni si compongono fra loro, i due gruppi sono in sostanza identici. Ora andiamo a dimostrare che ad un gruppo finito qualsiasi G di m

operazioni può sempre sostituirsi un gruppo Γ oloedricamente isomorfo di m sostituzioni sopra m lettere.

Siano 1) $S_1\ S_2\ S_3 \cdots S_m$

le m operazioni di G; se le moltiplichiamo tutte da una medesima parte, p. es. a destra, per una di esse S_i otteniamo le m operazioni

2) $S_1S_i\ ,\ S_2S_i\ ,\ S_3S_i \cdots S_mS_i$

le quali, in altro ordine, sono le m operazioni 1) stesse. Dalla permutazione 1) degli m oggetti $S_1\ S_2\ S_3 \cdots S_m$ si passa alla permutazione 2) con una sostituzione sulle m lettere S che indichiamo con

$$\gamma_i = \begin{pmatrix} S_1S_i, & S_2S_i \cdots & S_mS_i \\ S_1 & S_2 \cdots\cdots & S_m \end{pmatrix}$$

Le m sostituzioni γ_i $(i = 1, 2 \cdots m)$ sopra le m lettere S formano un gruppo Γ oloedricamente isomorfo con G. — E infatti se ne componiamo due γ_i, γ_k fra loro abbiamo

$$\gamma_i\gamma_k = \begin{pmatrix} S_1(S_iS_k), & S_2(S_iS_k), & \cdots S_m(S_iS_k) \\ S_1 & S_2 & \cdots\cdots S_m \end{pmatrix}$$

e se supponiamo

$$S_iS_k = S_j$$

questa è precisamente la γ_j. — Si noti poi che T ha l'ordine precisamente eguale al numero delle lettere su cui opera ed è semplicemente transitivo. Dunque: A qualunque gruppo finito di m operazioni si può porre in corrispondenza d'isomorfismo oloedrico un gruppo semplicemente transitivo su m lettere. —

Così è dimostrato quanto avevamo asserito al §6, che cioè lo studio dei gruppi di sostituzioni sopra lettere include in sostanza quello apparentemente più generale dei gruppi qualsiasi (finiti) di operazioni. —

§10. — **Sottogruppi invariantii.** — Sia G un gruppo di sostituzioni d'ordine m:

$$G = (S_1, S_2, \ldots\ldots S_m)$$

e τ una sostituzione qualunque. — Le m sostituzioni trasformate delle S

$$\tau^{-1}S_1\tau, \quad \tau^{-1}S_2\tau, \quad \ldots\ldots \quad \tau^{-1}S_m\tau$$

formano evidentemente (§5) un nuovo gruppo T; questo dicesi il gruppo trasformato di G per mezzo della τ e si scrive $T = \tau^{-1}G\tau$. —

I due gruppi G, T sono in sostanza identici, mutata la denominazione delle lettere. — Può anche accadere che il gruppo trasformato coincida assolutamente con G ed allora si dice che **la sostituzione τ è permutabile col gruppo G**. — Ciò avviene in particolare se τ è permutabile con tutte le sostituzioni di G.

Ora sia G un gruppo e T un suo sottogruppo; se trasformiamo T con una sostituzione qualunque g di G, otteniamo un gruppo trasformato

$$T' = g^{-1} T g$$

che è evidentemente un nuovo sottogruppo di G. — Se accade che T sia permutabile con tutte le sostituzioni di G, tutti i sottogruppi trasformati di T coincidono con T, e T stesso dicesi un **sottogruppo invariante** o **eccezionale** in G.(*) Così ad esempio il gruppo alterno è un sottogruppo invariante del gruppo totale. — Un altro esempio lo troviamo dato dal teore-

---

(*) Noi adotteremo la prima denominazione che è ormai la più usata e che è stata introdotta da Lie nella teoria dei gruppi continui. —

ma seguente:

Se G è un gruppo in isomorfismo meriedrico d'ordine m col gruppo T, quel sottogruppo

$$\Sigma = (\sigma_1 \sigma_2 \ldots \sigma_m)$$

di G costituito da quelle sostituzioni che corrispondono all'identità in T è un sottogruppo invariante in G.

E infatti se g è una qualunque sostituzione di G, γ la corrispondente in T alla

$$g^{-1}\sigma_i g \qquad (i = 1, 2, \ldots m)$$

corrisponde

$$\gamma^{-1} \cdot 1 \cdot \gamma = 1$$

e però

$$g^{-1}\sigma_i g = \sigma_k$$

È importante osservare una proprietà che è in certo modo l'inversa di quella ora osservata e che consiste in ciò: Se il gruppo G possiede un sottogruppo invariante

$$\Sigma = (\sigma_1 \sigma_2 \ldots \sigma_m)$$

d'ordine m, esso è in isomorfismo meriedrico d'ordine m con un gruppo T, all'identità in T corrispondendo Σ in G.

Sia $n = rm$ l'ordine di G e riportiamo le sue sostituzioni, rispetto al sottogruppo Σ, nel quadro con r orizzontali

$$G = \begin{cases} \sigma_1 , \ \sigma_2 \ldots\ldots \sigma_m \\ \sigma_1 t_2 , \ \sigma_2 t_2 , \ \ldots\ldots \sigma_m t_2 \\ \ldots\ldots\ldots\ldots\ldots \\ \sigma_1 t_r , \ \sigma_2 t_r , \ \ldots\ldots \sigma_m t_r \end{cases}$$

Siccome per qualunque valore degli indici i, k si ha

$$t_k^{-1} \sigma_i t_k = \sigma_j$$

avendo l'indice j un conveniente valore, cioè

$$\sigma_i t_k = t_k \sigma_j ,$$

se supponiamo

$$t_\alpha t_\beta = \sigma_i t_\gamma$$

avremo

$$(\sigma_i t_\alpha)(\sigma_k t_\beta) = \sigma_i \sigma_j t_\alpha t_\beta = \sigma_l t_\gamma$$

Questo ci dimostra che: moltiplicando fra di loro due qualunque sostituzioni del quadro G il numero d'ordine della orizzontale cui appartiene la sostituzione prodotto dipende unicamente da quelli delle orizzontali cui appartengono rispettivamente le due componenti.

Ora se moltiplichiamo tutte le sostituzioni di G per

una medesima di $\mathcal{G}$, le $n = \tau m$ sostituzioni del quadro non fanno che permutarsi fra loro (cf § 15) e l'osservazione precedente dimostra che le τ orizzontali del quadro si permutano fra loro come sistemi di imprimitività.—
Se indichiamo con lettere (simboli) le τ orizzontali e sieno

$$\Lambda_1\ \Lambda_2\ \Lambda_3 \ldots\ldots\ldots \Lambda_\tau$$

ad ogni sostituzione g di $\mathcal{G}$ verrà così a corrispondere una sostituzione γ sulle Λ. E si vede subito che le γ costituiranno appunto un gruppo Γ d'ordine τ, col quale $\mathcal{G}$ si troverà in isomorfismo meriedrico d'ordine m, all'identità in Γ corrispondendo il sottogruppo invariante Σ in $\mathcal{G}$.—

§17.— Gruppi semplici e composti.—

Ogni gruppo $\mathcal{G}$ possiede due sottogruppi invarianti e cioè $\mathcal{G}$ stesso e l'identità. Se non ammette alcun altro sottogruppo invariante il gruppo si dice **semplice**, altrimenti **composto**. Per i gruppi composti hanno grande importanza le loro serie di composizione di cui ora dobbiamo occuparci. Ma prima conviene dimostrare alcuni lemmi, cominciando dal seguente teorema:

A) Siano $\mathfrak{G}, \mathfrak{G}'$ due gruppi dei rispettivi ordini m, m' e fra di loro permutabili nel senso che ciascuno di essi sia permutabile con tutte le sostituzioni dell'altro; se μ è l'ordine del sottogruppo T comune a $\mathfrak{G}, \mathfrak{G}'$ moltiplicando tutte le sostituzioni di $\mathfrak{G}$ per tutte quelle di $\mathfrak{G}'$ si otterranno solo $\frac{m m'}{\mu}$ sostituzioni diverse che formeranno un gruppo H contenente $\mathfrak{G}, \mathfrak{G}'$ come sottogruppi invarianti e in questi T sarà contenuto alla sua volta come sottogruppo invariante.

Pongasi

$$\Gamma = (\gamma_1\ \gamma_2 \cdots\cdots \gamma_n)$$

$$m = n n \qquad m' = n n'$$

e si distribuiscano le sostituzioni g, g' di $\mathfrak{G}, \mathfrak{G}'$ nei quadri

$$\mathfrak{G} = (\Gamma t_1, \Gamma t_2 \qquad \Gamma t_n) \qquad (t_1 = 1)$$

$$\mathfrak{G}' = (\Gamma t'_1, \Gamma t'_2 \qquad \Gamma t'_{n'}) \qquad (t'_1 = 1)$$

essendo g, g' due sostituzioni qualunque l'una in $\mathfrak{G}$, l'altra in $\mathfrak{G}'$ si ha che la sostituzione

$$g g' \cdot g^{-1} g'^{-1} = (g g' g^{-1}) g'^{-1}$$

appartenendo per ipotesi $g g' g^{-1}$ a $\mathfrak{G}'$, appartiene essa

stessa a $\mathfrak{G}'$; ma d'altronde scrivendola invece

$$g\cdot(g'\bar{g}'g^{-1})$$

si vede che appartiene anche a $\mathfrak{G}$, onde sarà una so=
stituzione γ del sottogruppo comune $\mathfrak{T}$, cioè

$$1)\qquad gg'=\gamma_i g'g\ ;$$

in parole: due sostituzioni di $\mathfrak{G}$, $\mathfrak{G}'$ sono permu=
tabili a meno di una sostituzione del sotto=
gruppo comune $\mathfrak{T}$.

Ciò premesso avendosi per un prodotto qualunque gg'

$$\gamma_i T_\alpha\cdot\gamma_k T'_\beta=(\gamma_i T_\alpha\gamma_k)\,T'_\beta=\gamma_j T_\gamma T'_\beta$$

si vede che questi prodotti daranno al massimo le

$\mu\nu\nu'=\frac{m m'}{\mu}$ sostituzioni distinte

$$2)\qquad \gamma_i T_\alpha T'_\beta \qquad \begin{cases} i=1,2,\dots\dots\mu \\ \alpha=1,2,\dots\dots\nu \\ \beta=1,2,\dots\dots\nu' \end{cases}$$

Ma queste sono effettivamente distinte, poichè da

$$\gamma_i T_\alpha T'_\beta=\gamma_k T_a T'_b$$

seguirebbe

$$(\gamma_k T_a)^{-1}(\gamma_i T_\alpha)=T'_b T'^{-1}_\beta$$

onde la sostituzione del 2° membro che è in $\mathfrak{G}'$ sarebbe anche in $\mathfrak{G}$ e però in $\mathfrak{T}$ ciò che è assurdo se non è $T'_b=T'_\beta$, onde si trae per $T_a=T_\alpha$, $\gamma_i=\gamma_k$ —.

Che le $\frac{m m'}{\mu}$ sostituzioni 2) formino un gruppo H resulta

subito applicando la 1) poichè si ha

$$(gg')(g_1 g_1') = g(g'g_1)g_1' = gg_1(g_1^{-1}g'g_1)g_1' = (gg_1)(g_1^{-1}g'g_1)g_1' = g_2 g_2'$$

Ora $\mathfrak{G}$ è invariante in H poichè

$$(gg')^{-1}\mathfrak{G}(gg') = g'^{-1}(g^{-1}\mathfrak{G}g)g' = g'^{-1}\mathfrak{G}g' = \mathfrak{G}$$

e similmente $\mathfrak{G}'$ è invariante in H. — L'ultima parte del teorema risulta poi immediatamente.

Un sottogruppo invariante $\mathfrak{G}$ di un gruppo T dicesi massimo se non esiste in T alcun altro sottogruppo invariante contenente $\mathfrak{G}$.

Ora può darsi benissimo che un gruppo T possegga due diversi sottogruppi eccezionali massimi $\mathfrak{G}$, $\mathfrak{G}'$ ed a questo proposito dimostriamo l'importante teorema:

B) Se un gruppo T possiede due diversi sottogruppi eccezionali massimi $\mathfrak{G}, \mathfrak{G}'$, il sottogruppo Σ comune a $\mathfrak{G}, \mathfrak{G}'$ è eccezionale massimo tanto in $\mathfrak{G}$ che in $\mathfrak{G}'$ ed ha rispetto a $\mathfrak{G}$ l'indice che $\mathfrak{G}'$ ha in T e rispetto a $\mathfrak{G}'$ l'indice di $\mathfrak{G}$ in T.

È chiaro intanto che $\mathfrak{G}$ sarà permutabile con tutte le sostituzioni di $\mathfrak{G}'$ come $\mathfrak{G}'$ con tutte quelle di $\mathfrak{G}$ e potremo quindi applicare il teorema precedente. Indicando con m, m', μ i rispettivi ordini di $\mathfrak{G}, \mathfrak{G}', \Sigma$, il gruppo H for-

nato dal combinare fra loro le sostituzioni di G, G' è certo contenuto in T ma d'altronde contenendo G, G' come sottogruppi invariantì dovrà coincidere con T; altrimenti G, G' non sarebbero massimi in T come abbiamo supposto.(*) Dunque T è di ordine uguale a $\frac{mm'}{\mu}$ e però l'indice di G in T è precisamente dato da $\frac{m'}{\mu}$ come l'indice di Σ in G' e similmente l'indice di G' in T è uguale a $\frac{m}{\mu}$ come l'indice di Σ in G. — Resta solo a dimostrarsi che Σ è un variante massimo in G, G'. Se è possibile sia Δ un sottogruppo invariante in G e contenente Σ; in primo luogo si vede subito per la 1) che Δ è permutabile con tutte le sostituzioni di G', come evidentemente G' con tutte quelle di Δ. — Applicando nuovamente il teorema A) e combinando le sostituzioni di G' con quelle di Δ otterremmo un sottogruppo invariante di T contenente G', che non sarebbe dunque massimo.

§18. — Serie di composizione. Teorema di Jordan.

Sia G un gruppo, G_{n-1} suo sottogruppo invariante massimo,

(*) Si osservi che questa conclusione vale anche se si suppone soltanto uno dei due gruppi p. es. G invariante massimo in T.

$\mathfrak{G}_1$ un sottogruppo invariante massimo di $\mathfrak{G}$, e così via fin chè si arrivi all' identità 1; la serie dei gruppi

2) $$\mathfrak{G}\ \mathfrak{G}_1\ \mathfrak{G}_2\ \mathfrak{G}_3 \ldots\ldots \mathfrak{G}_{r-1}\ 1$$

formata in guisa che ciascun gruppo sia sottogruppo invariante massimo rispetto a quello che lo precede dicesi una serie di **composizione** del gruppo $\mathfrak{G}$. Se il gruppo è semplice, la serie di composizione consta naturalmente dei due soli gruppi

$$\mathfrak{G},\ 1\ .$$

Indichiamo con e_1 l' indice di $\mathfrak{G}_1$ in $\mathfrak{G}$, con e_2 l' indice di $\mathfrak{G}_2$ in $\mathfrak{G}_1$ ..... con e_r l' indice di 1 in $\mathfrak{G}_{r-1}$ (cioè l' ordine di $\mathfrak{G}_{r-1}$); i numeri

$$e_1\ e_2 \ldots\ldots e_r$$

dicansi i **fattori di composizione** della serie 2)

Ora sussiste il teorema dovuto a Jordan:

Due serie di composizione di un medesimo gruppo $\mathfrak{G}$ hanno sempre, prescindendo dall'ordine, i medesimi fattori di composizione.

S'intende quindi che questi numeri $e_1\ e_2 \ldots\ldots e_r$ sono inerenti alla natura del gruppo, onde possono dirsi i fattori di composizione del gruppo.

Per dimostrare il teorema di Jordan ammettiamo che sia

vero per tutti i gruppi d'ordine inferiore a m e dimostriamo che è vero anche per i gruppi G d'ordine m; sic come per $m = 1, 2$ il teorema è subito verificato, così sarà provato in generale.

Consideriamo due diverse serie di composizione per G e siano

a) $G \; G_1 \; G_2 \; G_3 \ldots\ldots\ldots\ldots 1$

b) $G \; G_1' \; G_2' \; G_3' \ldots\ldots\ldots\ldots 1$

coi rispettivi fattori di composizione

$$e_1 \; e_2 \; e_3 \ldots\ldots\ldots\ldots$$

$$e_1' \; e_2' \; e_3' \ldots\ldots\ldots\ldots$$

Se indichiamo con Σ il sottogruppo comune a G_1, G_1' che sono sottogruppi invariantivi massimi in G, potremo applicare il teorema B) del paragrafo precedente onde indicando con

$$\Sigma \; \Sigma_1 \; \Sigma_2 \ldots\ldots 1$$

una serie di composizione di Σ, nelle due serie

a') $G \; G_1 \; \Sigma \; \Sigma_1 \; \Sigma_2 \ldots\ldots 1$

b') $G \; G_1' \; \Sigma \; \Sigma_1 \; \Sigma_2 \ldots\ldots 1$

avremo due nuove serie di composizione di G. Ora per il teorema B) i due primi fattori di composizione della serie a') sono

$$e_1 \qquad e_1'$$

e quelli di b')

e_1' e_1

e poichè da Σ in poi queste due serie evidentemente coincidono esse hanno i medesimi fattori di composizione. D'altra parte le due serie a) a') avendo i due primi gruppi a comune hanno certo gli stessi fattori di composizione poichè abbiamo ammessa vera la proprietà pei gruppi come G_1, d'ordine inferiore all'ordine m di G; lo stesso dicasi delle due serie b) b'), onde il teorema di Jordan risulta dimostrato.

Come corollario del teorema di Jordan si osservi che in due diverse serie di composizione di un gruppo il numero dei gruppi della serie è lo stesso.

§19. — **Serie di composizione di gruppi isomorfi.** — Due gruppi G, T oloedricamente isomorfi hanno gli stessi fattori di composizione, poichè ad ogni sottogruppo di G corrisponde un sottogruppo di T e se il primo è invariante in G il secondo è invariante in T; se dunque

$$G, G_1, G_2, \ldots\ldots G_{r-1}\ 1$$

è una serie di composizione di G, i gruppi corrispon-

denti $\Gamma, \Gamma_1, \Gamma_2 \ldots\ldots, \Gamma_{r-1}\ 1$

formeranno una serie di composizione di T. Supponiamo ora che G sia un isomorfismo meriedrico d'ordine m con T e sia

$$\Sigma = (\sigma_1\ \sigma_2 \ldots\ldots \sigma_m)$$

il sottogruppo di G che corrisponde all'identità in T. Se poniamo, come al §14

$$G = \begin{cases} \Sigma t_1 & (t_1 = 1) \\ \Sigma t_2 \\ \ldots\ldots \\ \Sigma t_q \end{cases}$$

e chiamiamo

$$\gamma_1\ \gamma_2 \ldots\ldots \gamma_q$$

le sostituzioni di γ corrispondenti a quelle delle varie orizzontali, supposto $\gamma_i \gamma_k = \gamma_j$

avremo altresì $(\sigma_\alpha t_i)(\sigma_\beta t_k) = \sigma_\gamma t_j$

Di qui risulta che ad ogni sottogruppo T' di T corrisponde in G un sottogruppo G' in isomorfismo meriedrico d'ordine m con T' e G' sarà invariante in G se T' lo è in T; di più se T' è invariante massimo in T, G' sarà invariante massimo in G.

Se dunque

$$\Gamma\ \Gamma_1\ \Gamma_2 \ldots\ldots \Gamma_{r-1}\ 1$$

è una serie di composizione di T e

$$G\ G_1\ G_2 \ldots\ldots G_{r-1}\ \Sigma$$

la corrispondente serie in $\mathfrak{G}$, vidi

$$\Sigma \quad \Sigma_1 \quad \Sigma_2 \quad \ldots \quad \Sigma_{r-1} \quad 1$$

una serie di composizione di Σ, sarà evidentemente

$$\mathfrak{G} \quad \mathfrak{G}_1 \ldots\ldots \mathfrak{G}_{r-1} \quad \Sigma \quad \Sigma_1 \ldots\ldots \Sigma_{r-1} \quad 1$$

Dunque: I fattori di composizione di $\mathfrak{G}$ risultano dall'associare quelli di $\mathfrak{T}$ coi fattori di composizione di Σ.

§20.– Sottogruppi invarianti del gruppo totale.– Quando è dato un gruppo una delle più importanti ricerche da farsi è quella della sua composizione e noi qui vogliamo appunto esaminare tale quistione pel gruppo totale $\mathfrak{G}$ di sostituzioni sopra n lettere. Abbiamo già osservato che esso contiene come sottogruppo invariante il gruppo alterno, ma possiamo dimostrare: Eccettuato il caso di $n=4$, il gruppo totale sopra n lettere non ammette alcun sottogruppo eccezionale all'infuori del gruppo alterno.–

Sia infatti $\mathfrak{T}$ un sottogruppo eccezionale di $\mathfrak{G}$; $\mathfrak{T}$ sarà permutabile con qualunque sostituzione sopra le n lettere e però se contiene una sostituzione conterrà anche

tutte le simili. Se dunque T non coincide col gruppo alterno, non potrà pel teorema al §8 contenere alcuna sostituzione circolare. Ora fra le sostituzioni di T scegliamone una S che sposti il minor numero possibile di elementi e sia

$$S = (a\,b\ldots)(c\,d\ldots)(e\,f\ldots)\ldots,$$

dove, per quanto precede, il numero dei cicli sarà almeno 2; T conterrà anche la sostituzione simile

$$S' = (a\,b\ldots)(c\,d\ldots)^{-1}(e\,f\ldots)^{-1}\ldots$$

e però anche

$$S\,S' = (a\,b\ldots)^2,$$

la quale, se non fosse $(a\,b\ldots)^2 = 1$, sposterebbe meno lettere di S contro l'ipotesi. Tutti i cicli di S sono dunque del 2° ordine cioè

$$S = (a\,b)(c\,d)\ldots$$

Ma il numero dei cicli non può superare 2, perchè se si avesse

$$S = (a\,b)(c\,d)(e\,f)\ldots$$

anche

$$S_1 = (a\,c)(b\,d)(e\,f)\ldots$$

sarebbe in T e però anche

$$S_1 S = (a\,d)(b\,c)$$

che sposta meno elementi di S.

Avremo dunque $S = (a\,b)(c\,d)$;

ma se $n > 4$ vi sarà una 5ª lettera e $\mathfrak{T}$ conterrà quindi anche

$$S_2 = (a\,e)(c\,d)$$
$$S_2 S = (a\,c\,b)$$

che sposta meno elementi di S.–

Siccome per $n = 2, 3$ il teorema si verifica subito, così è stabilito in generale. Pel caso $n = 4$, non potendo il gruppo T contenere alcuna sostituzione circolare non avrà altre sostituzioni all'infuori del prodotto di due trasposizioni; esso è quindi necessariamente il gruppo

$$T = 1, (a\,b)(c\,d), (a\,c)(b\,d), (a\,d)(b\,c)$$

il quale è effettivamente invariante nel gruppo totale.–

§21.– Semplicità del gruppo alterno

per $n > 4$.– Resta ora che ricerchiamo la serie di composizione del gruppo alterno T.– La questione è risolta dall'importante teorema: **Per $n > 4$ il gruppo alterno è semplice.**–

Come si vedrà nelle applicazioni della teoria dei gruppi alle equazioni algebriche, questo teorema equivale all'altro: **Le equazioni generali di grado superiore al quarto sono risolubili per radicali.**

Per dimostrare il teorema enunciato indichiamo con

$$G \quad T \quad H$$

il gruppo totale su n lettere, il gruppo alterno ed un sottogruppo invariante massimo di quest'ultimo. Poichè H non è invariante in G, se indichiamo con t una sostituzione dispari, p. es. una trasposizione, il gruppo

$$H_1 = t^{-1} H t$$

sarà diverso da H ed invariante massimo in $t^{-1} T t = T$. — Pel teorema B) del § 17 il sottogruppo Σ comune ad H, H_1 sarà invariante in T ed indicando con m l'ordine di H, H_1 avrà un ordine x dato da

$$x = \frac{m^2}{1/2\,\pi(n)}$$

Ora Σ sarebbe invariante non solo in T ma ben anche in G poichè, essendo σ una qualunque sostituzione di Σ la sostituzione

$$t^{-1} \sigma t$$

si trova sì in $H_1 = t^{-1} H t$ che in $H = t^{-1} H_1 t$. —

Pel teorema al § precedente avremo dunque $x = 1$ cioè

$$3 \cdot 4 \cdot 5 \cdots\cdots n = m^2$$

Ora, giovandosi di un teorema sulla frequenza dei numeri primi;(*) sarebbe facile dimostrare che ciò è assurdo il

(*) Il teorema che dice: Se x è un numero intero, fra

il prodotto $3 \cdot 4 \cdot 5 \cdots\cdots n$ non potendo mai essere un quadrato. Ma anche senza far uso di questo teorema possiamo completare la nostra dimostrazione osservando che per $n = 5$ il gruppo alterno è semplice perchè

$$3 \cdot 4 \cdot 5 = 60$$

non è un quadrato, e dimostrando che il gruppo alterno su n lettere $(n > 5)$ è semplice se lo è quello su $n-1$ lettere.. Ora osserviamo che il sottogruppo invariante supposto H di T è certamente transitivo poichè se decomponiamo una sostituzione qualunque S di H in cicli

$$S = (a\ b \cdots\cdots) \cdots\cdots$$

e con α, β indichiamo due lettere qualunque fra le n, essendo T $n-2 > 2$ volte transitivo esiste in T una sostituzione

$$U = \begin{pmatrix} \alpha & \beta \cdots\cdots \\ a & b \cdots\cdots \end{pmatrix}$$

quindi in H la

$$U^{-1} S U = (\alpha\ \beta \cdots\cdots)$$

che porta la lettera arbitraria α nella arbitraria β. Ciò posto, le sostituzioni di T che lasciano ferma una determinata lettera p. es. a, formano il gruppo alterno sulle $n-1$ lettere rimanenti e quelle di H che lasciano ferma

---

τ e $2\tau - 2$ è compreso almeno un numero primo.—

a un sottogruppo invariante H_1 di T_1; dunque per la nostra ipotesi H_1 sarà l'identità. Il teorema al principio del § 10 sui gruppi transitivi dimostra che l'ordine di H sarebbe uguale a n e però si avrebbe

$$3.4.5.\ldots\ldots n = n^2,$$

ciò che è evidentemente assurdo.

Dai teoremi dimostrati risulta che la serie di composizione del gruppo totale per $n > 4$ si compone unicamente del gruppo stesso, del gruppo alterno e della identità e perciò i fattori di composizione sono

$$2 \quad \text{e} \quad \tfrac{1}{2}\pi(n).$$

Per $n = 4$ abbiamo la serie di composizione

$$\underline{G}_{24} \text{ (gruppo totale)}$$
$$\underline{G}_{12} \text{ (gruppo alterno)}$$
$$\underline{G}_4 = \big(1, (ab)(cd), (ac)(bd), (ad)(bc)\big)$$
$$\underline{G}_2 = \big(1, (ab)(cd)\big)$$
$$\underline{G}_1 = 1$$

coi fattori di composizione

$$2, 3, 2, 2.$$

Quanto ai casi $n = 2, 3$ essi rientrano nel caso generale.

22. Serie di composizione principale.—

Torniamo ora ai teoremi generali sulle serie di composizione dei gruppi ed in primo luogo facciamo l'osservazione seguente: Se G_r è un sottogruppo invariante di G esiste sempre una serie di composizione di G contenente G_r.—

Sia infatti G_1 un sottogruppo invariante massimo di G contenente G_r, nel quale adunque G_r sarà invariante, in G_2 un sottogruppo invariante massimo di G_1 contenente G_r e così via; formeremo così i primi termini di una serie di composizione che da G va a G_r e basterà poi prolungarla con una serie di composizione di G_r per avere una serie di composizione di G in cui figura G_r. Ora osserviamo in una serie di composizione di G, avverrà in generale che un gruppo intermedio della serie sarà bensì invariante nel gruppo che lo precede ma in generale non in G.— Ma possiamo anche formare una serie

$$c) \quad G, H, J, K, \ldots\ldots 1$$

così composta che ciascun gruppo sia sottogruppo del precedente ed invariante in G, né fra due termini consecutivi della serie per es. J, K sia possibile inserire un sottogruppo di J invariante in G e contenente K; una tal

rie c) si dirà una serie principale.. È chiaro co
me da una serie principale c) possa formarsi un'ordinaria
serie di composizione

d) $G\ H\ H_1\ H_2 \ldots\ldots H_\nu\ J\ J_1\ J_2 \ldots\ldots J_\mu\ K \ldots\ldots$

inserendo fra due gruppi consecutivi della c) una serie di com
posizione del primo gruppo che contenga il secondo. Ora di
siamo che: Se fra due termini successivi del
la serie principale c) sono inseriti i gruppi

$$H\ H_1 \ldots\ldots\ldots H_\nu$$

per formare la serie di composizione d) i fat
tori di composizione da H fino a J sono tut
ti fra loro eguali..

A dimostrarlo basterà, pel teorema di Jordan, dedurre da
una serie di composizione, come d) nella quale il fatto e
nunciato si verifichi. Ora osserviamo che H, essendo inva
riante in H ma non in G, trasformato con tutte le so
stituzioni di G darà luogo ad un certo numero di gruppi
distinti

e) $H, H', H'', H''', \ldots\ldots$

quali tutti saranno sottogruppi invarianti massimi in H
contenenti J che sarà il loro massimo sottogruppo co
mune; inoltre i vari gruppi e) permutandosi fra loro gua

do si trasformano simultaneamente con una sostituzione di G, il loro sottogruppo comune Δ è invariante in G e contenendo J coincide con J stesso.—

Ora prendiamo p. es. H_1, H_1' e sia H_2 il loro sottogruppo comune; potremo cominciare la serie di composizione da H a J con

$$H \; H_1 \; H_2 \cdots\cdots J$$

o con

$$H \; H_1' \; H_2 \cdots\cdots J$$

e se applicando il teorema B) §14 indichiamo con p l'indice di H_1 (o H_1') in H sarà pure p l'indice di H_2 in H_1 (o H_1') onde se $H_2 = J$ avremmo appunto da H_1 a J due fattori di composizione uguali a p.— Se H_2 non coincide con J prendiamo fra i gruppi e) un gruppo H_1'' che non contenga H_2 e sia H_3 il sottogruppo comune di H_1, H_1'' H_1'''.— Così continuiamo finchè arriveremo necessariamente a J che è il massimo sottogruppo comune a tutti i gruppi e).—

Dobbiamo dimostrare che ciascun gruppo H_2 è invariante massimo nel precedente H_{2-1} col fattore costante p di composizione.— Ammettiamo la cosa vera per z gruppi

$$H_1 \; H_2 \cdots\cdots H_z$$

Atteniamo nel modo anzidetto e dimostriamo che è vera

anche pel successivo. Perciò essendo H_z il sottogruppo comune a $H_1\, H_1' \cdots H_1^{(z-2)}\, H_1^{(z-1)}$, H_{z+1} il sottogruppo comune a $H_1\, H_1' \cdots H_1^{(z-1)}\, H_1^{(z)}$ indichiamo con K_z il sottogruppo comune a

$$H_1\, H_1' \cdots H_1^{(z-2)}\, H_1^{(z)};$$

sarà K_z un vero sottogruppo di H_{z-1} perchè se coincidesse con H_{z-1} ne verrebbe che H_{z+1} coinciderebbe con H_z. Per ipotesi, nelle due serie di z termini

$$H_1\, H_2 \cdots H_{z-1}\, H_z$$
$$H_1\, H_2 \qquad H_{z-1}\, K_z$$

ciascun gruppo è sottogruppo invariante massimo nel precedente col fattore di composizione p. Ma allora essendo H_{z+1} il sottogruppo comune ai due gruppi H_z, K_z il teorema fondamentale B) § 14 ci dimostra che la proprietà si verifica anche per gli $z+1$ gruppi

$$H_1\, H_2 \cdots H_z\, H_{z+1} \qquad \text{c.d.d.}$$

In fine osserviamo che, se una serie principale

$$G\ H\ J \cdots\cdots 1$$

si chiamano fattori principali gli indici che hanno i vari gruppi nel gruppo precedente, applicando il solito teorema B) si dimostra facilmente che in due serie principali diverse i fattori principali, salvo l'ordine, sono sempre gli stessi.

§23.- Gruppi fattoriali e teorema di Hölder.

Al teorema di Jordan (§18) è stato portato da Hölder (*) un complemento essenziale che ora andiamo a vedere. Ma ritorniamo prima alla costruzione data al §16 di un gruppo T in isomorfismo meriedrico con un dato gruppo G in guisa che all'identità in T corrisponda in G un sottogruppo invariante assegnato

$$\Sigma = (\sigma_1\ \sigma_2 \cdots\cdots \sigma_m)$$

Il gruppo T, come lì si è detto, non è altro che il gruppo secondo il quale si permutano le r orizzontali del quadro

$$\left\{\begin{array}{llll} \sigma_1 & \sigma_2 & & \sigma_m \\ \sigma_1 t_2, & \sigma_2 t_2 & & \sigma_m t_2, \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_1 t_r & \sigma_2 t_r & & \sigma_m t_r \end{array}\right.$$

moltiplicando tutte queste sostituzioni per una qualunque di esse.- Chiameremo questo gruppo T il gruppo complementare di G rispetto al sottogruppo invariante Σ e lo indicheremo col simbolo di quoziente: $\frac{G}{\Sigma}$.-

Ora consideriamo una serie di composizione di un gruppo G, sia

$$G\ G_1\ G_2 \cdots\cdots G_{\nu-1}\ G_\nu \cdots\cdots ;$$

(*) Math. Annalen Bd. 34

e costruiamo i successivi gruppi complementari di ciascun gruppo della serie rispetto al seguente cioè i gruppi

$$\Gamma_1 = \frac{G}{G_1}, \quad \Gamma_2 = \frac{G_1}{G_2}, \ldots\ldots \Gamma_\nu = \frac{G_{\nu-1}}{G_\nu}, \ldots$$

questi li diremo con Hölder i gruppi fattoriali di G. Il teorema di Jordan si può allora enunciare dicendo che gli ordini dei gruppi fattoriali rimangono sempre gli stessi, comunque si varii la serie di composizione. Ora Hölder ha osservato, e in ciò appunto consiste il suo teorema, che: I gruppi fattoriali stessi non fanno che permutarsi fra loro variando la serie di composizione. In ciò naturalmente riguardiamo, secondo le osservazioni del § 15, come identici due gruppi che siano oloedricamente isomorfi.

Per dimostrare il teorema di Hölder basta riprendere il teorema B) del § 14 e completarlo nel modo seguente: Essendo $\mathfrak{G}$, $\mathfrak{G}'$ sottogruppi invariantì massimi in Γ e Σ il sottogruppo comune a $\mathfrak{G}$, $\mathfrak{G}'$, i due gruppi complementari

$$\frac{G}{\Sigma}, \quad \frac{\Gamma}{G'}$$

hanno, come in altro abbiamo veduto, eguale ordine; ma ora diciamo di più che essi sono, astrattamente considerati, identici, cioè oloedricamente isomorfi. Abbiamo in-

fatti $$\mathcal{G} = (\Sigma t_1, \Sigma t_2, \ldots\ldots \Sigma t_m)$$
$$\mathcal{G} = (\Sigma t'_1, \Sigma t'_2, \ldots\ldots \Sigma t'_{m'})$$
$$T = (\mathcal{G}' t_1 \; \mathcal{G}' t_2 \ldots\ldots \mathcal{G}' t_m)$$

e se supponiamo

$$t_i t_k = \sigma_{ik} t_j \; ; \quad (\Sigma t_i) t_k = \Sigma t_j \; ; \quad (\mathcal{G}' t_i) t_k = \mathcal{G}' t_j$$

il che, se si riflette al modo come i gruppi $\frac{\mathcal{G}}{\Sigma}$, $\frac{T}{\mathcal{G}'}$ sono formati, dimostra appunto il loro isomorfismo oloedrico. Completato così il teorema B) basta ripetere le considerazioni del §18 riferendole ai gruppi fattoriali anzichè ai loro ordini per stabilire il teorema di Hölder.—

§24.— **Gruppi complementari.**— La nozione di gruppo complementare $\frac{\mathcal{G}}{T}$ di un gruppo $\mathcal{G}$ rispetto ad un sottogruppo T può stabilirsi anche se T non è invariante in $\mathcal{G}$.— Supponiamo che sia q l'indice di

$$T = (g_1 \, g_2 \ldots\ldots g_n)$$

in $\mathcal{G}$ e poniamo

$$\mathcal{G} = (T t_1, T t_2, T t_3, \ldots\ldots T t_q) \quad (t_1 = 1)$$

Diciamo due sostituzioni g, g' di $\mathcal{G}$ **equivalenti** rispetto al sottogruppo T, quando sia

$$g' = \gamma g \, ,$$

essendo γ una sostituzione di T.— La nozione di equiva-

lenza è invertibile, come resulta dall'osservare che

$$g = s^{-1} g' s ;$$

inoltre è chiaro che due sostituzioni equivalenti ad una terza sono equivalenti fra loro (*). Si ottiene evidentemente un sistema completo di sostituzioni non equivalenti di G rispetto a T estraendo da ogni orizzontale del quadro costituito per G una sostituzione; per es. formano un tale sistema completo $t_1 t_2 \ldots t_q$.

Ora moltiplicando le q sostituzioni di un sistema completo a destra per una medesima sostituzione di g si otterrà ancora un sistema completo perchè se $g's$, $g''s$ sono equivalenti tali debbono essere anche g', g''. (**).

Dunque, moltiplicando a destra per g, le q classi di sostituzioni equivalenti, nelle quali si ripartono le sostituzioni di G, si permutano fra loro. Indicando con τ la corrispondente sostituzione sopra q classi, riguardate come elementi, vediamo subito che tutte le τ formano un gruppo poichè se a g, g' corrispondono rispettivamente τ, τ' al prodotto gg' corrisponde il prodotto $\tau\tau'$. Dunque:

(*) Da $g' = sg$, $g'' = sg$ segue $g'' = (sg')g'$.

(**) Da $g''s = sg's$ segue $g'' = sg'$.

Se un gruppo $\mathfrak{G}$ ammette un sottogruppo $\mathfrak{T}$ d'indice q ripartendo le sostituzioni di $\mathfrak{G}$ nelle q classi di sostituzioni equivalenti rispetto a $\mathfrak{T}$, si ottiene un gruppo di sostituzioni sulle q classi in isomorfismo (in generale meriedrico) con $\mathfrak{G}$.–

Indicheremo nuovamente questo gruppo con

$$H = \frac{\mathfrak{G}}{\mathfrak{T}}$$

e lo diremo il gruppo complementare di $\mathfrak{G}$ rispetto a $\mathfrak{T}$.– Come riconosceremo se l'isomorfismo di $\mathfrak{G}$ con H è oloedrico o meriedrico? Sia g una sostituzione di $\mathfrak{G}$ cui corrisponda l'identità in H .– Essendo S una qualunque sostituzione di $\mathfrak{G}$, dovremo avere

$$S_g = \gamma_i S$$

cioè

$$g = S^{-1} \gamma_i S$$

Dunque g dovrà appartenere a tutti i sottogruppi

$$S^{-1} \mathfrak{T} S$$

trasformati di $\mathfrak{T}$ per una qualunque sostituzione S di $\mathfrak{G}$, e viceversa se ciò accade, a g corrisponde l'identità in H .– Ne concludiamo: Alla sostituzione identica in $H = \frac{\mathfrak{G}}{\mathfrak{T}}$ corrisponde in $\mathfrak{G}$ il sottogruppo comune a tutti i sottogruppi trasformati di $\mathfrak{T}$.

L'isomorfismo sarà dunque oloedrico solo quando questo sottogruppo si riduce alla identità.

§25. Il primo Teorema di Sylow. Secondo il teorema fondamentale del §4 ogni sottogruppo di un gruppo G deve avere un ordine divisore dell'ordine m del gruppo. In generale però, se n è un divisore dell'ordine m del gruppo G, non si può asserire che esistano in G sottogruppi d'ordine n. Ma vi ha un caso molto importante, nel quale si può senz'altro concludere l'esistenza di un tale sottogruppo, quando cioè n sia la potenza di un numero primo p. Sussiste infatti il seguente teorema dovuto a Sylow:

Se l'ordine m di un gruppo G è divisibile per la potenza p^d di un numero primo p,(**) esiste in G qualche sottogruppo di ordine p^d.

Per dimostrarlo supporremo già provato che ogni gruppo, il cui ordine è divisibile per p^{d-1} contiene sottogruppi di

(**) Non occorre supporre che p^d sia la più alta potenza di p che divide m onde, pel teorema stesso, esisteranno in G anche sottogruppi degli ordini $p^{d-1}, p^{d-2} \ldots\ldots p$.

ordine $p^{\alpha+1}$ e faremo vedere come supponendo che il gruppo non abbia sottogruppi d'ordine p^α ne venga una contraddizione assurda.

Consideriamo l'insieme di tutte le sostituzioni di $\mathfrak{G}$ ciascuna delle quali è permutabile con ogni altra sostituzione di $\mathfrak{G}$ e siano

$$\sigma_1 \; \sigma_2 \; \ldots\ldots \; \sigma_m \; ,$$

queste sostituzioni (fra le quali figura l'identità) formeranno evidentemente un sottogruppo Σ.

Supponiamo dapprima che l'ordine m di Σ sia divisibile per p; allora dico in primo luogo che fra le sostituzioni di Σ se ne potrà scegliere una a periodo p. Per dimostrarlo indichiamo con

$$\tau_1 = 1 \; , \; \tau_2 \; , \; \ldots\ldots \; \tau_m$$

i rispettivi periodi di

$$\sigma_1 \; \sigma_2 \ldots\ldots \sigma_m$$

e costruiamo le $\tau_1 \times \tau_2 \times \tau_3 \ldots\ldots \times \tau_m$ sostituzioni di Σ

$$(A) \qquad \sigma_1^{\alpha_1} \sigma_2^{\alpha_2} \ldots\ldots \sigma_m^{\alpha_m} \qquad \begin{cases} \alpha_1 = 1, 2, \ldots\ldots \tau_1 \\ \alpha_2 = 1, 2, \ldots\ldots \tau_2 \\ \\ \alpha_m = 1, 2, \ldots\ldots \tau_m \end{cases}$$

Ciascuna σ si trova in (A) ripetuta lo stesso numero di volte, cioè quante volte viene $\sigma_1^{\alpha_1} \sigma_2^{\alpha_2} \ldots \sigma_m^{\alpha_m} = 1$,

onde il prodotto $\tau_1 \tau_2 \dots \tau_m$ sarà divisibile per α, quindi per p. Una delle τ, poniamo τ_i, è dunque divisibile per p e se poniamo

$$\sigma = \sigma_i^{\frac{\alpha_i}{p}}$$

otteniamo appunto una σ divisibile per p. Consideriamo il gruppo ciclico

$$T = (1, \sigma, \sigma^2, \dots, \sigma^{p-1})$$

e formiamo il gruppo complementare

$$H = \frac{G}{T}$$

di G rispetto a T. Il gruppo H di ordine uguale a $\frac{m}{p}$ è un isomorfismo meriedrico di ordine p con G; il suo ordine $\frac{m}{p}$ essendo divisibile per p^{k-1}, esisterà per ipotesi in H un sottogruppo H_1 d'ordine p^{k-1} e il corrispondente sottogruppo G_1 di G sarà appunto d'ordine p^k come si voleva.

Sia ora α non divisibile per p. Se diciamo affini due sostituzioni a, b di G quando esista in G almeno una sostituzione t che trasformi a in b (con che la t^{-1} trasformerà b in a) è chiaro che due sostituzioni affini ad una terza sono affini fra loro (*); potremo quindi

---

*) Da $t^{-1} a t = b$ $\tau^{-1} b \tau = c$ segue invero $\tau t^{-1} a t \tau^{-1} = (t\tau^{-1})^{-1} a (t\tau^{-1}) = c$

ripartire le sostituzioni di $\mathcal{G}$ in classi ponendo nella medesima classe quelle che sono affini fra loro. Ciascuna delle sostituzioni σ del sottogruppo Σ, e queste soltanto, forma per sè una classe. Ora da ciascuna classe prendiamo una sostituzione e sia così

$$(A) \qquad \sigma_1\ \sigma_2 \ldots\ldots \sigma_m\ t_1\ t_2 \ldots\ldots t_\nu$$

un sistema completo di sostituzioni non affini, cioè tale che ogni sostituzione di $\mathcal{G}$ risulti affine ad una ed una sola sostituzione del sistema (A).

Le sostituzioni di $\mathcal{G}$ permutabili con t_τ ($\tau = 1, 2, 3 \ldots \nu$) formano un sottogruppo $\mathcal{G}_\tau$ di $\mathcal{G}$, il cui ordine m_τ sarà un divisore puro di m (cioè $m_\tau < m$) perchè, nel caso contrario, la t_τ dovrebbe appartenere a Σ. Sia

$$\mathcal{G}_\tau = (g_1\ g_2 \ldots g_{m_\tau})$$

e posto

$$h_\tau = \frac{m}{m_\tau}$$

ripartiamo le sostituzioni di $\mathcal{G}$ rispetto a quelle di $\mathcal{G}_\tau$ nel quadro

$$\mathcal{G} = \begin{cases} \mathcal{G}_\tau \\ \mathcal{G}_\tau \cdot \tau_2 \\ \ldots \\ \mathcal{G}\ \tau_{b_\tau} \end{cases};$$

due sostituzioni di $\mathcal{G}$ trasformano t_τ nella medesima

sostituzione o in sostituzioni diverse secondo che appartengono o no alla medesima orizzontale nel quadro. Dunque vi sono in G precisamente h_2 sostituzioni affini a t_2 e poichè ogni sostituzione di G è affine ad una sola del sistema (A) risulta

$$m = n + \frac{m}{m_1} + \frac{m}{m_2} + \ldots\ldots + \frac{m}{m_\nu}.$$

Ora essendo m divisibile, n non divisibile per p, ma al meno dei quozienti $\frac{m}{m_i}$ dovrà essere non divisibile per p; sia $\frac{m}{m_2}$. Allora m_2 sarà, come m, divisibile per p^α. Se G_1, come supponiamo, non contiene sottogruppi d'ordine p^α, nemmeno potrà contenerli il suo sottogruppo G_2 il cui ordine $m_2 < m$ è ancora divisibile per p^α. Ma allora, per la stessa ragione, si troverebbe un divisore puro m_2' di m_2 ancora divisibile per p^α e si avrebbe una serie decrescente infinita di numeri interi positivi

$$m, m_2, m_2' \ldots\ldots$$

tutti divisibili per p^α, ciò che è assurdo. Così il teorema di Sylow è completamente dimostrato. È utile notare come suoi corollari i teoremi di Cauchy

1°) Se p^α è la più alta potenza del numero primo p che divide $\pi(n)$ (*), si può formare un gruppo d'ordine p^α su n let-

tore. Tale gruppo contiene sottogruppi degli ordini

$$p^{\alpha-1}\ p^{\alpha-2}\ \ldots\ldots\ p$$

2°) Se l'ordine di un gruppo G è divisibile pel numero primo p esiste nel gruppo qualche sostituzione a periodo p.-

Esiste infatti in G un sottogruppo T d'ordine p ed ogni sua sostituzione (l'identità esclusa) è a periodo p.-

§ 26.- Il secondo teorema di Sylow.- Dal teorema che abbiamo dimostrato nel § precedente, Sylow ha dedotte alcune importanti conseguenze di cui ora ci occuperemo.- Conviene perciò che facciamo alcune osservazioni preliminari.- Sia G un gruppo composto e

$$H = (S_1\ S_2\ \ldots\ S_n)$$

un suo sottogruppo invariante, g una sostituzione qualunque di G che non appartenga ad H e β il suo periodo.- Il minimo esponente positivo α per quale accade

---

(*) Come è noto questo esponente α è dato da

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \qquad + \left[\frac{n}{p^k}\right]$$

essendo $p^k < n < p^{k+1}$.-

che g^d appartenga ad H si dirà il periodo relativo di g rispetto ad H. Come al §2 si dimostra che una potenza g^m di g appartiene ad H solo quando m è multiplo di d onde si vede che il periodo relativo è sempre un divisore del periodo assoluto (*)

Ora formiamo le dn sostituzioni

$$S_i,\ S_i g,\ S_i g^2 \ldots\ldots S_i g^{d-1} \quad [i = 1, 2 \ldots n]$$

le quali sono evidentemente tutte distinte e di più formano un gruppo perchè (*)

$$(S_i g^a)(S_k g^b) = S_i S_l g^{a+b}$$

Così abbiamo dimostrato il lemma:

Se H è un sottogruppo invariante di ordine n in un gruppo G ed d il periodo relativo di una sostituzione g di G rispetto ad H, esiste in G un sottogruppo d'ordine dn contenente H.

Possiamo anche dire: Il periodo relativo di

(*) Quello che si è detto finqui vale manifestamente per qualunque gruppo H e qualunque sostituzione g presa all'infuori di H.

(*) Essendo $g^a S_k g^{-a} = S_l$, $g^a S_k = S_l g^a$

una sostituzione g di G rispetto ad un suo sottogruppo invariante H è sempre un divisore dell'indice di H in G.-

Ciò premesso, ritorniamo al teorema di Sylow e indicando con m l'ordine del gruppo G, sia p^α la più alta potenza del numero primo p che divide m di guisa che sia

$$m = k\,p^\alpha,$$

non essendo più k divisibile per p.- Esiste certamente in G qualche sottogruppo H di ordine p^α, e, come dimostreremo, tutti i sottogruppi di ordine p^α sono trasformati di uno di essi H per mezzo delle sostituzioni di G.- Onde precisare poi quanti di tali sottogruppi esistono in G consideriamo tutte quelle sostituzioni di G che sono permutabili con H; esse formano un sottogruppo T di G contenente H come sottogruppo invariante, sicchè l'ordine di T sarà

$$n = \delta\,p^\alpha$$

dove δ è un divisore di k.- Siano $\gamma_1\ \gamma_2 \ldots\ldots \gamma_n$ le sostituzioni di T; nessuna di esse all'infuori di quelle del sottogruppo H può avere per periodo una potenza di p, altrimenti il periodo relativo di una tale sostituzione γ_i

spetto ad H sarebbe dato da p^β (con $\beta \geq 1$) mentre pel lemma precedente dovrebbe dividere

$$\frac{k p^\alpha}{n} = \frac{k}{s} = q$$

che è primo con p. Ora riportiamo le sostituzioni di $\mathfrak{G}$ rispetto a quelle di T nel quadro

$$\mathfrak{G} = \begin{cases} T \\ T t_2 \\ T t_3 \\ \cdots \\ T t_q \end{cases}$$

Si vedrà subito che se g, g' sono due sostituzioni di $\mathfrak{G}$ i gruppi trasformati di H

$$g^{-1} H g \quad , \quad g'^{-1} H g'$$

coincidono o sono diversi, secondo che g, g' nel quadro superiore appartengono o no alla medesima orizzontale. Avremo dunque in $\mathfrak{G}$ precisamente q sottogruppi di ordine p^α trasformati di H e cioè

$$H_1 = H \ , \ H_2 = t_2^{-1} H t_2 \ , \ \cdots\cdots \ , \ H_q = t_q^{-1} H t_q \ .$$

Dopo di ciò andiamo a dimostrare il secondo teorema di Sylow che si enuncia:

Se p^α è la più alta potenza del numero primo p che divide l'ordine n di un gruppo $\mathfrak{G}$ e H uno dei suoi sotto-

gruppi d' ordine p^α, tutti gli altri saranno trasformati di H per mezzo di sostituzioni di G. Il loro numero sarà dato da $q = \frac{m}{\delta p^\alpha}$ essendo δp^α l' ordine del massimo sottogruppo di G che contiene H come sottogruppo invariante. Questo numero q è sempre della forma

$$q = \tau p + 1$$

§ 27. **Dimostrazione**. — Come nella dimostrazione del primo teorema abbiamo ripartito le sostituzioni di G, così ora ripartiamo i q gruppi

$$H_1 \; H_2 \; \ldots\ldots\ldots \; H_q$$

in classi di gruppi affini rispetto ad H dicendo due gruppi H affini quando l'uno è trasformato dell' altro per mezzo di una sostituzione h di $H = H_1$. Il primo gruppo H costituisce per sé una classe ma ciò non accade più per uno dei rimanenti. Ed infatti se per qualunque sostituzione h_i di H fosse

$$h_i^{-1} H_i h_i = H_i$$

ne verrebbe

$$h^{-1} E_i^{-1} H \times E_i h = E_i^{-1} H E_i$$

cioè

$$(t_i h t_i^{-1})^{-1} \cdot H \cdot (t_i h t_i^{-1}) = H$$

e la sostituzione $t_i h t_i^{-1}$ apparterrebbe a T quindi, avendo per periodo una potenza di p, ad H; dunque t_i trasformerebbe H in sè stesso contro l'ipotesi. Ora se dimostriamo che in ogni classe di gruppi affini H_i salvo la prima, vi è sempre un numero di gruppi divisibile per p sarà intanto dimostrata la congruenza

$$q \equiv 1 \pmod{p}$$

Perciò consideriamo un sottogruppo H_i differente da H_1 esso non può essere come si è visto permutabile con tutte le sostituzioni di H, però può esserlo con alcune di esse, le quali formeranno in H un sottogruppo H' d'ordine $p^{\alpha-\beta}$ con $\beta > 0$. Ora se poniamo

$$H = \begin{cases} H' \\ H'h_2 \\ H'h_3 \\ \cdots\cdots \\ H'h_{p^\beta} \end{cases}$$

vediamo che due sostituzioni di H trasformano H_i in due gruppi coincidenti o distinti secondo che appartengono o non appartengono alla medesima orizzontale nel quadro superiore. Il numero dei gruppi affini ad H_i (H_i compreso) è dunque dato da p^β e però un mul-

tiplo di p, c. d. d.

Per dimostrare in fine che oltre i q gruppi H non esiste in G alcun altro sottogruppo di ordine p^α, supponiamo che un tale sottogruppo R esista. Distribuiamo i $q = zp+1$ gruppi H in classi di gruppi affini rispetto a R; poichè in ogni classe che abbia più di un gruppo ne esiste un numero multiplo di p, almeno una classe dovrà contenere un solo gruppo, sia H_i. Allora indicando con k una qualunque sostituzione di R si ha

$$k^{-1} H_i k = H_i ,$$

cioè

$$t_i k^{-1} t_i^{-1} . H . t_i k t_i^{-1} = H$$

dunque

$$t_i k t_i^{-1}$$

trasformando H in se medesimo appartiene a T, ed avendo per periodo una potenza di p, ad H stesso, dunque

$$R = t_i^{-1} H t_i = H_i \qquad \text{c. d. d.}$$

Si osserverà che in quest' ultima dimostrazione se avessimo supposto l' ordine di R una potenza di p inferiore a p^α ne avremmo concluso che R è necessariamente un sottogruppo di uno dei gruppi

$$H_1 \; H_2 \cdots\cdots H_q .$$

§28.- Gruppi di ordine p^{α}.- Per una ragione, che impareremo a conoscere trattando le applicazioni della teoria dei gruppi, diconsi risolubili quei gruppi i cui fattori di composizione sono numeri primi.- Un importante esempio di gruppi risolubili ci è fornito dai gruppi il cui ordine è la potenza di un numero primo.- Sussiste infatti il teorema

a) I fattori di composizione di un gruppo di ordine p^{n}, essendo p un numero primo, sono n fattori eguali a p.-

Per dimostrarlo stabiliremo l'altro teorema:

b) Un fattore di composizione di un gruppo qualsiasi non può mai eguagliare una potenza, diversa dalla prima, di un numero primo p.-

Da questo teorema segue evidentemente il primo poichè ogni fattore di composizione di un gruppo d'ordine p^{n} è necessariamente una potenza di p quindi uguale a p.-

Supponiamo, in opposizione al teorema enunciato b), che in un gruppo G esista un sottogruppo invariante massimo di T. d'indice uguale a p^{α}.- Se costruiamo

il gruppo complementare

$$H = \frac{G}{T}$$

esso sarà d'ordine p^α e sarà un gruppo semplice perchè, a causa dell'isomorfismo di H con G, al sottogruppo invariante massimo T di G corrisponde in H l'identità (cf. § 19). Ora se ci riportiamo alla seconda parte della dimostrazione del 1° teorema di Sylow (§ 25) ed osserviamo che ripartendo le sostituzioni di H in classi di sostituzioni affini, ogni classe, salvo quella costituita dall'identità, contiene un numero di sostituzioni eguali ad una potenza di p, ne verrebbe l'uguaglianza assurda

$$p^\alpha = 1 + p^a + p^b + \dots\dots$$

con $\quad \alpha > 1 \,, \quad a \geq 1 \,, \quad b \geq 1 \,, \dots\dots$

Si conoscono altri casi in cui dall'ordine del gruppo si può immediatamente concludere che si tratta di un gruppo risolubile. Così il teorema seguente deriva immediatamente dal secondo teorema di Sylow:

Un gruppo G di ordine uguale a pq, essendo p, q numeri primi, è un gruppo risolubile. E infatti sia p. es. $p > q$ (*); in G esiste un

(*) Per $p = q$ il teorema è già stato sopra dimostrato.

sottogruppo H almeno d' ordine $= p$, ma non ne può esistere più di uno perchè il loro numero r dovrebbe essere $\equiv 1 \pmod p$ ed eguagliare nello stesso tempo un divisore di $q < p$, onde $r = 1$. – Dunque H è invariante (massimo) in G, i cui fattori di composizione sono dunque p e q. – Ulteriori teoremi del genere di quelli ora stabiliti sono dovuti a Frobenius (*), ma noi qui ci limiteremo ad enunciarli:

1°) Ogni gruppo il cui ordine è il prodotto di fattori primi diversi è un gruppo risolubile. –

2°) Ogni gruppo di ordine $p^n q$, ove p, q sono numeri primi è un gruppo risolubile. –

§29. – Gruppi semplici degli ordini da 1 a 100. – Come si è visto nel § precedente vi sono certamente dei numeri interi che non possono mai figurare come fattori di composizione di un gruppo e sarebbe importante poter riconoscere le leggi relati-

(*) Setzungsberichte der Berliner Akademie Mai 1893. – V.i anche: Weber. – Algebra, II° Vol pag: 129 e seguenti. –

se ai fattori di composizione dei gruppi. Osserviamo che la ricerca dei possibili fattori di composizione di un gruppo coincide con quella dei possibili ordini dei gruppi semplici, giacchè appunto i gruppi fattoriali di un gruppo G sono gruppi semplici i cui ordini coincidono coi fattori di composizione di G. È chiaro che qualsiasi fattore primo p può assumersi come un fattore di composizione, ossia come ordine di un gruppo semplice, perchè se si prende una sostituzione ciclica su p lettere le sue potenze formano appunto un gruppo d'ordine p. In mancanza di ricerche generali, si sono ricercati i numeri più bassi che possono figurare come fattori di composizione. Così Hölder e Cole hanno esaurita la ricerca pei numeri fino a 500 ed hanno trovato (oltre ai numeri primi) come effettivi possibili effettivi fattori di composizione soltanto i tre seguenti

$$60, \quad 168, \quad 360$$

Di questi i due estremi ci sono già noti come ordini rispettivi dei gruppi alterni sopra 5 e sopra 6 elementi e fra breve troveremo anche un gruppo semplice di 168 sostituzioni (gruppo modulare).

mi vogliamo soltanto far vedere che non esistono gruppi semplici di ordine composto ≤ 100 fuori che appunto un gruppo di ordine 60..

In queste ricerche è essenziale ricordare il secondo teorema di Sylow ed osservare di più che se il gruppo G è semplice i q sottogruppi d'ordine p^α

$$H_1 \; H_2 \cdots\cdots H_q$$

trasformati con tutte le sostituzioni di G si permuteranno fra loro secondo le sostituzioni di un gruppo oloedricamente isomorfo (*) e transitivo sui q elementi H..

Ciò premesso, se si esaminano i numeri compresi da 1 a 100 e si applicano i teoremi del § 26 e le osservazioni precedenti, facilmente si vede (**) che non restano, come possibili ordini ai gruppi semplici che i due numeri

$$60 \;,\; 90 \;..$$

---

*) Se l'isomorfismo fosse meriedrico G sarebbe necessariamente composto.-

**) Se un gruppo G d'ordine $70 = 7 \cdot 10$ è necessariamente composto perchè il numero q dei suoi sottogruppi T di 7° ordine dev'essere un divisore di 10 e soddisfare la congruenza $q \equiv 1 \pmod 7$, onde $q = 1$ e però T è invariante in G..

L'ultimo ordine si esclude colle osservazioni seguenti.
Essendo $90 = 5 \cdot 18$ il numero q dei sottogruppi del 5° ordine in G dovrebbe essere un divisore di 18 e inoltre $q \equiv 1 \pmod 5$ onde $q = 6$; esisterebbe quindi un gruppo T_{90} transitivo primitivo su 6 lettere. Quelle sostituzioni di T che lasciano ferma una determinata lettera formerebbero quindi (§ 10) un sottogruppo H_{15} d'ordine 15 su 5 lettere. Ma ciò è impossibile poichè, pel teorema di Sylow H_{15} dovrebbe contenere un solo sottogruppo del 5° ordine, generato dunque dalle potenze di una sostituzione ciclica

$$S = (a\ b\ c\ d\ e)\ .$$

sulle 5 lettere; inoltre dovrebbe contenere una sostituzione U del 3° ordine che dovrebbe quindi spostare ciclicamente tre lettere e lasciar ferme le altre due. Sostituendo ad S, ove occorra una sua potenza potremo evidentemente supporre che queste due lettere siano d, e e si abbia $U = (a\ b\ c)$; (*)
Ora U trasforma S in $(b\ c\ a\ d\ e)$ che non è una potenza di S.—

(*) Se fosse $U = (a\ c\ b)$ basterebbe considerare U^2 in luogo di U.—

50.- Gruppi semplici d'ordine uguale a 60.-

mostriamo ora che: I gruppi semplici d'ordine
apportengono tutti ad un medesimo tipo,
sono tutti oloedricamente isomorfi fra
no e col gruppo alterno su 5 lettere.-

gruppo semplice d'ordine G_{60} contiene, per teorema
Sylow, precisamente 6 sottogruppi

$$H_1 \quad H_2 \quad H_3 \quad H_4 \quad H_5 \quad H_6$$

5° ordine ed è quindi oloedricamente isomorfo con un
uppo T_{60} transitivo sopra 6 lettere.-

osserviamo che le sostituzioni di T_{60} sono necessaria
nte tutte pari perchè nel caso opposto le sostituzioni
ri di T formerebbero un sottogruppo invariante di or
ine 30, mentre T è semplice.- Dunque T è un sot
gruppo del gruppo alterno $\mathfrak{G}$ d'ordine 360 sulle 6
ere.- L'indice di T in $\mathfrak{G}$ essendo = 6 il gruppo com
lementare $H = \frac{\mathfrak{G}}{T}$ è un gruppo oloedricamente isomor
o a $\mathfrak{G}$ sulle 6 classi

$$\Lambda_1 \quad \Lambda_2 \quad \Lambda_3 \quad \Lambda_4 \quad \Lambda_5 \quad \Lambda_6$$

in cui si ripartiscono le sostituzioni di $\mathfrak{G}$ rispetto a T
(62h): dunque H è il gruppo alterno sulle Λ.-

Al sottogruppo T_{60} in $\mathfrak{G}$ corrisponde un sottogruppo T' in

eguale ordine in H. — Ma le sostituzioni di T, se si prende per prima classe Λ, quella che comprende appunto tutte le sostituzioni di T, lasciano evidentemente Λ, inalterata onde T' è il gruppo alterno sulle 5 rimanenti Λ il che dimostra appunto il nostro teorema. —

§ 31. — **Gruppi Abeliani** — Dopo aver trattato delle principali proprietà dei gruppi generali volgiamoci ora allo studio di gruppi particolari importanti ed occupiamoci in primo luogo dei gruppi le cui sostituzioni (operazioni) sono due a due permutabili. — Tali gruppi diconsi **Abeliani**; essi godono di proprietà particolari, che non hanno luogo pei gruppi generali le cui operazioni non obbediscono alla legge commutativa. —

Sia G un gruppo Abeliano d'ordine n e

$$g_1 \quad g_2 \cdots\cdots g_n$$

le sue sostituzioni. — Ci proponiamo di dimostrare che si può sempre scegliere un certo numero r di sostituzioni del gruppo, siano

$$1) \qquad s_1 \quad s_2 \cdots\cdots s_r$$

in guisa che indicando con $\beta_1 \beta_2 \cdots \beta_r$ i loro ri-

spettivi periodi e costruendo le sostituzioni

$$2)\qquad s_1^{\gamma_1} s_2^{\gamma_2} \dots s_2^{\gamma_2} \quad \begin{cases} \gamma_1 = 0, 1, 2, \dots \beta_1 - 1 \\ \gamma_2 = 0, 1, 2, \dots \beta_2 - 1 \\ \dots\dots\dots\dots \\ \gamma_2 = 0, 1, 2, \dots \beta_2 - 1 \end{cases}$$

si ottengono tutte le sostituzioni del gruppo, a ciascuna una sola volta onde seguirà naturalmente

$$n = \beta_1 \beta_2 \dots \beta_2 .$$

Un tal sistema 1) di sostituzioni generatrici del gruppo si dirà una base del gruppo.

Perveniamo alla dimostrazione dell'esistenza di una base pel gruppo Abeliano G fondandoci sulle osservazioni seguenti:

1°) Il periodo del prodotto di più sostituzioni $g_1 g_2 \dots g_k$ del gruppo è un divisore del minimo multiplo comune dei singoli periodi di $g_1 g_2 \dots g_k$.

È infatti se m è questo minimo multiplo comune, a causa della permutabilità delle sostituzioni di G si ha

$$(g_1 g_2 \dots g_k)^m = g_1^m g_2^m \dots g_k^m = 1 .$$

2°) Se si decompone l'ordine n nel prodotto di due fattori $n_1 n_2$ primi fra loro

esiste in G un sottogruppo

$$A = (a_1\ a_2 \ldots\ldots a_{n_1})$$

di ordine n_1 ed un sottogruppo

$$B = (b_1\ b_2 \ldots\ldots b_{n_2})$$

di ordine n_2 tali che le sostituzioni

$$a_i\, b_k \quad \begin{cases} i = 1, 2, \ldots\ldots n_1 \\ k = 1, 2, \ldots\ldots n_2 \end{cases}$$

riproducono tutte le sostituzioni del gruppo G (*).—

Indichiamo con $a_1\ a_2\ a_3 \ldots\ldots$ tutte le sostituzioni di G che hanno per periodo un divisore di n_1. A causa della prima proprietà osservata, esse formano un sottogruppo A e noi dobbiamo dimostrare che il suo ordine n_1' è precisamente uguale a n_1.— Similmente le sostituzioni $b_1\ b_2\ b_3 \ldots\ldots$ che hanno per periodo un divisore di n_2 formano un sottogruppo B il cui ordine n_2' vogliamo dimostrare $= n_2$.—

(*) Naturalmente nei prodotti $a_i b_k$ non vi possono essere sostituzioni ripetute come risulta dall'osservare che A, B non hanno sostituzioni comuni, salvo l'identità, mentre da

$$a_i b_k = a_j b_l$$

seguirebbe

$$a_j^{-1} a_i = b_l b_k^{-1}\ -$$

Ora essendo g una qualunque sostituzione di $\mathfrak{G}$ e risolvendo in numeri interi α, β l'equazione

$$n_1\alpha + n_2\beta = 1$$

possiamo scrivere

$$g = g^{n_2\beta} \cdot g^{n_1\alpha}$$

Ma la sostituzione $g^{n_2\beta}$ essendo $(g^{n_1\beta})^{n_1} = g^{n\beta} = 1$ ha per periodo un divisore di n_1 e però è una sostituzione di A e similmente $g^{n_1\alpha}$ è una sostituzione b_k di B. - Dunque qualunque sostituzione g di $\mathfrak{G}$ si può decomporre in un prodotto $g = a_i b_k$

Le sostituzioni $a_i b_k$ essendo in numero di $n_1' n_2'$ si ha quindi 3) $n = n_1 n_2 = n_1' n_2'$

Ora n_1' è primo con n_2 perchè, se p fosse un loro divisore primo comune, esisterebbe in A una sostituzione a periodo p divisore di n_2 e dovrebbe quindi essere anche in B. - Così pure n_2' è primo con n_1 e però dalla 3) segue $n_1' = n_1$, $n_2' = n_2$ c. d. d.

È chiaro che se conoscessimo una base del gruppo Abeliano A ed una base del gruppo Abeliano B, le sostituzioni dell'una e dell'altra base riunite darebbero una base del gruppo prodotto

$$\mathfrak{G} = AB.$$

§ 32 – Base di un gruppo Abeliano –

Decomponiamo l'ordine n di un gruppo Abeliano nei suoi fattori primi e sia

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots \dots p_z^{\alpha_z},$$

essendo $p_1, p_2 \dots p_z$ i fattori primi diversi di n. Per quanto precede, potremo decomporre G nel prodotto

$$G = A_1 \; A_2 \dots \dots A_z$$

di z gruppi Abeliani dei rispettivi ordini

$$p_1^{\alpha_1}, \; p_2^{\alpha_2}, \dots \dots p_z^{\alpha_z}$$

come risulta anche del resto direttamente dal teorema di Sylow e dalla permutabilità delle sostituzioni del gruppo. Al nostro scopo basterà dunque dimostrare che: **Ogni gruppo Abeliano il cui ordine p^α è la potenza di un numero primo p possiede una base.** Da un tale gruppo G_{p^α} si possono certamente scegliere un certo numero di sostituzioni

$$s_1 \; s_2 \dots \dots s_z$$

i cui rispettivi ordini indichiamo con

$$p^{\alpha_1} \; p^{\alpha_2} \dots \dots p^{\alpha_z}$$

in guisa che nella serie

$$A) \qquad s_1^{\beta_1} \; s_2^{\beta_2} \dots \dots s_z^{\beta_z} \qquad (\beta_i = 0, 1, 2 \dots p^{\alpha_i - 1}$$

siano comprese tutte le sostituzioni di G, bastando, se

non altro, prendere per $s_1 s_2 \ldots s_z$ tutte le sostituzioni di G. – Ma in generale accadrà che fra le $p_1^{\alpha_1+\alpha_2+\cdots+\alpha_z}$ sostituzioni 4) se ne trovino delle ripetute; però, ove ciò accada, ogni sostituzione, come si è già osservato al §15, si troverà ripetuta il medesimo numero h di volte. – Fra i sistemi $s_1 s_2 \ldots s_z$ che possono scegliersi (il cui numero è finito) ve ne sarà certo uno almeno, pel quale questo numero h avrà il minimo valore possibile e noi vogliamo appunto provare che per questo minimo valore di h si ha $h=1$. Supponiamo se è possibile $h>1$ cioè

$$\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_z > \alpha$$

e sia

$$5) \qquad s_1^{\gamma_1} s_2^{\gamma_2} \ldots s_z^{\gamma_z} = 1$$

una delle sostituzioni che ripetono l'identità, essendo almeno una delle γ_1 poniamo γ_1 positiva $< p^{\alpha_1}$, siano

$$p^{u_1}, p^{u_2} \ldots p^{u_z}$$

le massime potenze di p che dividono rispettivamente

$$\gamma_1, \gamma_2 \ldots \gamma_z$$

e supponiamo le γ così ordinate che sia

$$u_1 \leq u_2 \leq u_3 \ldots \leq u_z \quad (*)$$

(*) Si noti bene che alcune delle u possono anche essere nulle.

La sostituzione

$$6) \qquad \tau = s_1^{\frac{\gamma_1}{p^{\alpha_1}}} \; s_2^{\frac{\gamma_2}{p^{\alpha_1}}} \qquad\qquad s_2^{\frac{\gamma_2}{p^{\alpha_1}}}$$

appartiene a $\mathcal{G}$ e il suo periodo è un divisore di p^{α_1} e però $< p^{\alpha_1}$ giacchè abbiamo supposto $\gamma_1 \not\equiv 0 \pmod{p^{\alpha_1}}$.. D'altronde essendo q una soluzione della congruenza

$$\frac{\gamma_1}{p^{\alpha_1}} \cdot q \equiv 1 \pmod{p^{\alpha_1}},$$

ed elevando la 6) alla potenza q otteniamo

$$s_1 = \tau^q s_2^{-q\frac{\gamma_2}{p^{\alpha_1}}} \cdots s_2^{-q\frac{\gamma_2}{p^{\alpha_1}}}$$

onde si vede che s_1 può ottenersi come combinazione di

$$7) \qquad \tau_1 \, s_2 \, s_3 \ldots s_2$$

Sostituendo quindi al sistema $s_1 s_2 \ldots s_2$ il sistema 7) otteniamo ancora, combinando le potenze di queste sostituzioni 4) tutte le sostituzioni del gruppo; ma poichè

$$p^{\alpha_1} p^{\alpha_2} \ldots p^{\alpha_2} < p^{\alpha_1} p^{\alpha_2} \ldots p^{\alpha_2}$$

il numero h è ridotto minore, contro l'ipotesi che avesse già il minimo valore possibile..

È chiaro che il processo medesimo che ci ha servito per la dimostrazione dell'esistenza di una base 6) potrebbe anche servire per la sua effettiva ricerca abbassando successivamente il valore di h fino a ridurlo $= 1$..

Dall'esistenza di una base $B = [s_1 s_2 \ldots s_2]$

pel gruppo possiamo trarre subito il teorema:
Ogni gruppo Abeliano è un gruppo risolubile. — Basterà per ciò mostrare che se p è un divisore primo dell'ordine n di un gruppo Abeliano G esisterà in G un sottogruppo G_1 d'indice uguale p poichè, a causa della permutabilità delle sostituzioni, sarà certo G_1 invariante in G. — Ora p divide certamente il periodo di una delle sostituzioni s_i della base, poniamo quello di s_1; allora combinando fra loro le potenze delle sostituzioni

$$s_1^p, s_2, s_3 \ldots s_r$$

si ottiene evidentemente il sottogruppo G_1 domandato (*). —

§ 33. — Invarianti di un gruppo Abeliano. — Un gruppo Abeliano può possedere diverse basi ed il numero degli elementi della base può an-

---

(*) Lo stesso teorema risulta anche immediatamente dalla decomposizione di un gruppo Abeliano nel prodotto di più gruppi Abeliani i cui ordini sono potenze di numeri primi e dal teorema del § 28. —

che variare da una base ad un'altra.-

Così p. es. se U, V sono due sostituzioni permutabili l'una di periodo m, l'altra di periodo n e supponiamo m, n primi fra loro, combinando le potenze di U con quelle di V si ottiene un gruppo G di ordine $n = mn$ pel quale le due sostituzioni U, V formano una base. Ma lo stesso gruppo può anche generarsi completamente colle sole potenze dell'unica sostituzione UV che è di periodo mn.- Però se noi decomponiamo prima il gruppo Abeliano d'ordine $n = p_1^{a_1} p_2^{a_2} \ldots\ldots$ nel prodotto dei gruppi parziali di ordini

$$p_1^{a_1}, p_2^{a_2} \ldots\ldots$$

e per ciascuno di questi cerchiamo una base col processo del § precedente possiamo dimostrare che il numero degli elementi nella base e i periodi delle rispettive sostituzioni restano sempre gli stessi, comunque si muti la base.- Questi numeri diconsi per ciò oppurtunamente gli **invarianti del gruppo** (**).-

Dobbiamo dunque dimostrare che se un gruppo Abeliano G d'ordine p^m possiede due diverse basi $[s_1, s_2, s_3, \ldots\ldots]$

(**) Weber - Algebra II pag. 39

$[\sigma_1\ \sigma_2\ \sigma_3 \ldots \sigma_q]$ le due basi constaranno di un medesimo numero d'elementi $z = q$ ed anche i periodi delle rispettive sostituzioni, prescindendo dall'ordine, saranno gli stessi. Indichiamo con

$$p^{\alpha_1},\ p^{\alpha_2},\ \ldots\ldots\ p^{\alpha_z}$$

i periodi delle sostituzioni della prima base e con

$$p^{\beta_1},\ p^{\beta_2},\ \ldots\ldots\ p^{\beta_q}$$

quelli delle sostituzioni della seconda onde sarà

$$\alpha_1 + \alpha_2 + \ldots\ldots + \alpha_z = \beta_1 + \beta_2 + \ldots\ldots + \beta_q = n$$

e supponiamo gli elementi delle basi così ordinati che si abbia $\alpha_1 \geq \alpha_2 \geq \alpha_3 \ldots\ldots$

$$\beta_1 \geq \beta_2 \geq \beta_3 \ldots\ldots$$

dimostreremo che si ha necessariamente

$$\alpha_1 = \beta_1\ ,\quad \alpha_2 = \beta_2\ ,\quad \alpha_3 = \beta_3 \ldots\ldots$$

Intanto poichè ogni sostituzione di G è una combinazione delle S, il più alto periodo di una sostituzione di G è dato da p^{α_1}; ma se ricorriamo invece alla seconda base vediamo che il più alto periodo è p^{β_1} onde risulta $\alpha_1 = \beta_1$. Ora supponiamo già dimostrato che si ha $\alpha_1 = \beta_1\quad \alpha_2 = \beta_2 \ldots\ldots \alpha_{i-1} = \beta_{i-1}$ e proviamo che sarà anche

$$\alpha_i = \beta_i$$

Sia invece se è possibile $\alpha_i < \beta_i$. Formiamo le potenze p^{α_i} di tutte le sostituzioni di $\mathcal{G}$ e vediamo quante sostituzioni diverse si ottengono in $\mathcal{G}$. Essendo U una qualunque sostituzione di $\mathcal{G}$ ed esprimendola per la prima base si ha

$$U = S_1^{\gamma_1} S_2^{\gamma_2} \dots S_{i-1}^{\gamma_{i-1}} S_i^{\gamma_i}$$

onde

$$U^{p^{\alpha_i}} = S_1^{\gamma_1 p^{\alpha_i}} S_2^{\gamma_2 p^{\alpha_i}} \dots S_{i-1}^{\gamma_{i-1} p^{\alpha_i}}$$

Le sostituzioni diverse in $\mathcal{G}$ di questa forma sono in numero di $p^{\alpha_1 + \alpha_2 + \dots + \alpha_{i-1} - (i-1)\alpha_i}$

D'altronde esprimendo U per la seconda base

$$U = \sigma_1^{\delta_1} \sigma_2^{\delta_2} \dots \sigma_{i-1}^{\delta_{i-1}} \sigma_i^{\delta_i} \dots$$

si ha

$$U^{p^{\alpha_i}} = \sigma_1^{\delta_1 p^{\alpha_i}} \sigma_2^{\delta_2 p^{\alpha_i}} \dots \sigma_{i-1}^{\delta_{i-1} p^{\alpha_i}} \sigma_i^{\delta_i p^{\alpha_i}} \dots$$

Ma per la medesima ragione di prima già il numero delle sostituzioni diverse nella serie

$$\sigma_1^{\delta_1 p^{\alpha_i}} \dots \dots \dots \sigma_{i-1}^{\delta_{i-1} p^{\alpha_i}}$$

è dato da $p^{\alpha_1 + \alpha_2 + \dots \alpha_{i-1} - (i-1)\alpha_i}$

onde dovremo avere $\sigma_i^{\delta_i p^{\alpha_i}} = 1$

qualunque sia δ_i, in particolare

$$\sigma_i^{p^{\alpha_i}} = 1$$

mentre abbiamo supposto che il periodo p^{β_i} di σ_i fos-

se maggiore di p^{di}.—

Dimostrato così il nostro teorema, possiamo dedurne il criterio per riconoscere se due gruppi Abeliani del medesimo ordine sono astrattamente identici, cioè oloedricamente isomorfi, o no.— Abbiamo infatti:

Due gruppi Abeliani sono identici se hanno eguali invarianti e viceversa.—

Se infatti gli invarianti dei due gruppi Abeliani sono identici basta agli elementi di una base dell'un gruppo far corrispondere elementi di egual periodo nella base dell'altro gruppo e i due gruppi sono posti in corrispondenza d'isomorfismo oloedrico.—

L'inversa si vede egualmente.—

§ 34.— Gruppi transitivi risolubili sopra un numero primo di elementi.—

Un'altra importante classe di gruppi è quella dei gruppi transitivi risolubili sopra un numero primo p di elementi di cui ora andiamo ad occuparci.— Sia G un tale gruppo e

$$G \quad G_1 \quad G_2 \ldots\ldots G_{n-1} \quad 1$$

una sua serie di composizione, i fattori di composizio-

ne, i fattori di composizione essendo numeri primi. - Dimostriamo in primo luogo che tutti i gruppi della serie, tranne l'identità, sono gruppi transitivi sulle p lettere. - Il primo essendo transitivo per ipotesi supponiamo che sia G_{i-1} transitivo G_i intransitivo; sia

$$a_1\ a_2 \ldots\ldots a_\mu$$

uno dei sistemi di transitività in cui si scindono le p lettere rispetto alle sostituzioni di G_i. - Se con b_1 indichiamo un'altra qualunque fra le p lettere esisterà in G_{i-1} (transitivo) una sostituzione S che porta a_1 in b_1 e come il gruppo G_i muove transitivamente le μ lettere a così $S^{-1} G_i S$ muterà transitivamente le lettere che S sostituisce ad

$$a_1\ a_2 \ldots\ldots a_\mu$$

Essendo $S^{-1} G_i S = G_i$ ne concludiamo che tutti i sistemi di transitività debbono contenere un egual numero μ di lettere e perciò μ è un divisore di p quindi di

$$\mu = p \quad \text{o} \quad \mu = 1$$

Nel 1° caso G_i sarebbe transitivo contro l'ipotesi,
nel 2° $G_i = 1$ c. d. d.

Ciò premesso, vediamo che il penultimo gruppo G_{m-1} dovendo essere transitivo deve avere un ordine divisibile

per p e poichè il suo ordine deve essere d'altronde un numero primo, sarà precisamente = p. — Esso conterrà cioè delle p potenze di una sostituzione ciclica S sulle p lettere e sarà dunque un gruppo ciclico

$$T = (1, S, S^2, \ldots S^{p-1})$$

Dimostriamo ora che questo penultimo gruppo T sarà invariante non solo nel gruppo precedente G_{n-2} ma ben anche in tutti i precedenti e in G. — Per ciò supponiamo che $G_{n-1} = T$ sia invariante in G_i e dimostriamo che lo sarà pure in G_{i-1}. — Essendo T invariante in G_{i-1} non esiste, pel teorema di Sylow (*), in G_{i-1} alcun altro sottogruppo di ordine p. — Ora se U è una qualunque sostituzione di G, essa trasforma T in un nuovo sottogruppo

$$U^{-1} T U$$

di G_{i-1}, che deve dunque coincidere con T c. d. d.

Per trovare dunque tutti i gruppi transitivi risolubili sopra un numero primo p di elementi dobbiamo ricercare i gruppi che contengono come sottogruppo invariante il gruppo ciclico T e basterà ricercare il

---

(*) È infatti la più alta potenza di p che divide l'ordine di G_{i-1} (divisore di $\pi(n)$) è la prima. —

più ampio di tali gruppi; il quale coi suoi sottogruppi darà tutti i gruppi richiesti.—

§35.— **Gruppo metaciclico.**— Il più ampio gruppo nel quale il gruppo ciclico

$$T = (1, S, S^2 \ldots S^{p-1})$$

è contenuto come sottogruppo invariante dicesi il gruppo **metaciclico** e noi vogliamo qui trovare tutte le sostituzioni del gruppo metaciclico ed in particolare determinarne l'ordine.— Indichiamo le p lettere con

$$x_0\ x_1\ x_2 \ldots \ldots x_{p-1}$$

e poniamo

$$S = (x_0\ x_1\ x_2 \ldots \ldots x_{p-1})$$

Ogni sostituzione Θ del gruppo metaciclico deve trasformare S in una potenza S^z di S talchè si abbia

$$\Theta^{-1} S \Theta = S^z;$$

viceversa, se ciò accade, Θ appartiene al gruppo metaciclico.— Qualunque poi sia $z \not\equiv 0 \pmod p$, S^z è simile ad S e però esistono sostituzioni Θ corrispondenti.— La sostituzione ciclica S^z si può scrivere in p modi diversi soltanto e però ogni sostituzione S^z dà luogo a p sostituzioni Θ differenti; se una di esse è Θ_1

le altre sono $S\tau_1, S^2\tau_1, \ldots S^{p-2}\tau_1$

e poichè τ assume i $p-1$ valori $1, 2, 3, \ldots p-1$ abbiamo intanto il risultato:

Il gruppo metaciclico contiene $p(p-1)$ sostituzioni.

Se scriviamo S^τ in un determinato modo facendo cominciare il suo ciclo con x_0, come S, è chiaro che le $p-1$ sostituzioni corrispondenti

$$\tau_1 = 1, \tau_2, \tau_3, \ldots \tau_{p-1}$$

lasceranno ferma x_0 e le sostituzioni del gruppo metaciclico $G_{p(p-1)}$ si ripartiranno nel quadro

$$\begin{cases} 1, S, S^2, \ldots S^{p-1} \\ \tau_2, S\tau_2, S^2\tau_2, \ldots S^{p-1}\tau_2 \\ \ldots\ldots\ldots\ldots\ldots \\ \tau_{p-1}, S\tau_{p-1}, S^2\tau_{p-1}, \ldots S^{p-1}\tau_{p-1} \end{cases}$$

Fra queste soltanto quelle della prima verticale lasciano ferma x_0 e però formano in $G_{p(p-1)}$ un sottogruppo d'ordine $p-1$. È facile vedere che questo sottogruppo è ciclico cioè formato dalle potenze di una sostituzione ciclica sulle $p-1$ lettere $x_1 x_2 \ldots x_{p-1}$. Riguardiamo infatti gli indici delle lettere come aventi non un valore assoluto ma solo un valore rispetto al no-

tulo p talchè le lettere x_m, x_n coincidano quando $m \equiv n \pmod p$. Se indichiamo allora con g una radice primitiva $(\mathrm{mod}\ p)$ la sostituzione T_g che trasforma

$$S = (x_0\ x_1\ x_2 \ldots x_{p-1})$$

in

$$S^g = (x_0\ x_g\ x_{2g} \ldots x_{(p-1)g})$$

avrà l'espressione

$$T_g = \begin{pmatrix} x_0 & x_g & x_{2g} & \cdots & x_{(p-1)g} \\ x_0 & x_1 & x_2 & \cdots & x_{p-1} \end{pmatrix}$$

e decomposta in cicli darà un solo ciclo

$$T_g = (x_1\ x_g\ x_{g^2} \ldots x_{g^{p-2}}).$$

Le $p(p-1)$ sostituzioni del gruppo metaciclico sono dunque date dalla formola

$$U = S^\beta T^\alpha \qquad \begin{cases} \alpha = 0, 1, 2 \ldots p-2 \\ \beta = 0, 1, 2 \ldots p-1 \end{cases}$$

Vediamo in quale potenza di S la S è trasformata dalla $S^\beta T^\alpha$. L'effetto di S^β su qualunque indice ν è di aggiungervi β e quello di S^α di moltiplicare per g^α, onde $S^\beta b^\alpha$ si può scrivere simbolicamente

$$U = S^\beta T^\alpha = \begin{pmatrix} (\nu+\beta)\, g^\alpha \\ \nu \end{pmatrix}.$$

Ora scrivendo S così:

$$S = (x_{-\beta},\ x_{-\beta+1} \ldots x_{p-\beta-1})$$

e trasformando con U otteniamo

$$U^{-1} S\, U = (x_0\ x_{g^\alpha}\ x_{2g^\alpha} \ldots x_{(p-1)g^\alpha}) = S^{g^\alpha}$$

In particolare avremo dunque

$$T^{-\alpha} S^{\beta} T^{\alpha} = S^{\beta g^{\alpha}} = S^{\beta_1}$$

ove $$\beta_1 \equiv \beta g^{\alpha} \pmod p$$

quindi $$S^{\beta} T^{\alpha} = T^{\alpha} S^{\beta_1}$$

Il gruppo metaciclico è quindi anche dato dalle $p(p-1)$ sostituzioni

$$T^{\alpha} S^{\beta_1} \quad \begin{cases} \alpha = 0, 1, 2, \ldots . p-2 \\ \beta_1 = 0, 1, 2 \ldots . p-1 \end{cases}$$

§ 30.– Rappresentazione analitica delle sostituzioni del gruppo metaciclico.–

L'effetto di una sostituzione $S^{\beta} T^{\alpha}$ di $G_{p(p-1)}$ è, come abbiamo visto di portare ogni indice ν nell'indice

$$\nu' \equiv g^{\alpha} \nu + \beta g^{\alpha} \pmod p$$

Se poniamo $g^{\alpha} = a$ $\beta g^{\alpha} = b$, il primo numero a percorrerà un sistema completo di resti (mod p) escluso lo zero ed il secondo tutto un tale sistema.– Possiamo dunque rappresentare analiticamente il gruppo metaciclico colla formola

$$(1) \qquad \nu' \equiv a\nu + b \pmod p \quad \begin{cases} a = 1, 2, \ldots . p-1 \\ b = 0, 1, 2 \ldots p-1 ; \end{cases}$$

il gruppo ciclico T_p corrisponderà evidentemente al valore $a = 1$.–

Come già abbiamo visto al § 9 de soltanto le sostituzioni di T_p fra quelle del gruppo metaciclico hanno per periodo e le altre hanno per conseguenza a periodo un divisore di p.–

Possiamo confermare ciò direttamente e trovare quale è effettivamente il periodo di una sostituzione (1) quando $a \not\equiv 1 \pmod p$. Se chiamiamo $\mathcal{U}$ la sostituzione (1) e facciamo le sue potenze troviamo

per $\mathcal{U}^2$ $\quad v' \equiv a^2 v + (a+1)b$

per $\mathcal{U}^3$ $\quad v' \equiv a^3 v + (a^2+a+1)b \pmod p$

. . . . . .

per $\mathcal{U}^\delta$ $\quad v' \equiv a^\delta v + (a^{\delta-1} + a^{\delta-2} + \ldots + a + 1)b$

Perchè risulti $\mathcal{U}^\delta = 1$ è evidentemente necessario che sia

$$a^\delta \equiv 1 \pmod p$$

ma tale condizione è anche sufficiente perchè da

$$a^\delta - 1 = (a-1)(a^{\delta-1} + a^{\delta-2} + \ldots + 1) \equiv 0 \pmod p$$

segue $\quad a^{\delta-1} + a^{\delta-2} + \ldots + 1 \equiv 0 \pmod p$.

Dunque: Le sostituzioni (1) del gruppo metaciclico con $a \not\equiv 1 \pmod p$ hanno per periodo l'esponente δ cui appartiene $a \pmod p$, quelle con $a \equiv 1 \pmod p$ hanno per periodo p.-

Osserviamo che: Il gruppo metaciclico è doppiamente transitivo.- È infatti se i, k sono due indici qualunque la sostituzione

$$v' \equiv (k-i)v + i \pmod p$$

porta gli indici $0, 1$ rispettivamente in i, k.- Come si

vede l'ordine del gruppo metaciclico $p(p-1)$ è il minimo compatibile col suo doppio grado di transitività.–

Delle due sostituzioni S, T generatrici del gruppo metaciclico la prima è pari e la seconda è dispari e quindi fra le sostituzioni $S^\beta T^\alpha$ del gruppo sono pari quelle con α pari e dispari quelle con α dispari.–
Nella rappresentazione analitica (1) sono pari quelle in cui a è residuo quadratico (mod p), dispari quelle in cui a è non residuo. Le pari formano un sottogruppo d'ordine $\frac{p(p-1)}{2}$ che dicesi il gruppo semimetaciclico.–

§ 37.– **Serie di composizione del gruppo metaciclico**.– Servendoci della formula (§ 35)

$$(2) \qquad S^\beta T^\alpha = T^\alpha S^{\beta_1} \qquad (\beta_1 \equiv \beta g^\alpha \pmod p)$$

facilmente troviamo una serie di composizione pel gruppo metaciclico osservando che se δ è un divisore qualunque di $p-1$ le $p\delta$ sostituzioni

$$S^\beta T^{\frac{p-1}{\delta}\tau} \qquad \begin{cases} \tau = 0, 1, 2 \ldots \delta-1 \\ \beta = 0, 1, 2 \ldots p-1 \end{cases}$$

formano un sottogruppo invariante in $G_{p(p-1)}$.–

È invero le (3) formano un gruppo perchè, a causa della (2), si ha

$$S^{\beta}Z^{\frac{p-1}{\delta}z}S^{\beta'}Z^{\frac{p-1}{\delta}z'} = S^{\beta+\beta'}Z^{-\frac{p-1}{\delta}z}Z^{\frac{p-1}{\delta}(z+z')}$$

Questo gruppo è invariante in $G_{p(p-1)}$ perchè posto

$$U = S^{\beta'}Z^{\alpha'}$$

si ha $U^{-1}S^{\beta}Z^{\frac{p-1}{\delta}z}U = Z^{-\alpha'}S^{\beta+\beta'}Z^{\frac{p-1}{\delta}z}S^{\beta'}Z^{\alpha'} =$

$$= S^{\gamma}Z^{\frac{p-1}{\delta}z}S^{\beta'}Z^{\alpha} = S^{\gamma}Z^{\frac{p-1}{\delta}z}S^{\beta} \quad (*)$$

Se indichiamo poi con p_1 un divisore primo qualunque di δ le $\frac{p\delta}{p_1}$ sostituzioni

$$S^{\beta}Z^{\frac{p-1}{\delta}\cdot z} \qquad \begin{cases} z = 0, 1, \ldots \frac{\delta}{p_1}-1 \\ \beta = 0, 1, 2 \ldots p-1 \end{cases}$$

formano nel precedente gruppo $G_{p\delta}$ un sottogruppo in

---

(*) Si può anche verificare la proprietà sulla rappresentazione analitica $v' \equiv av + b$ osservando che, chiamando a il moltiplicatore della sostituzione, il moltiplicatore del prodotto di due sostituzioni è eguale al prodotto dei moltiplicatori. Perciò se facciamo percorrere a b tutti i valori (mod p) e ad a quelli che soddisfano la congruenza $a^{\delta} \equiv 1$ otterremo appunto un sottogruppo invariante nel gruppo metaciclico.—

variante d' indice primo = p.

Ora se scindiamo $p-1$ nei suoi fattori primi eguali o no, si

$$p-1 = p_1 p_2 \cdot \cdots \cdot p_z$$

potremo formare una serie di gruppi

$$G_{p(p-1)} \quad G_{\frac{p(p-1)}{p_1}} \quad G_{\frac{p(p-1)}{p_1 p_2}} \cdots \cdots G_{\frac{p(p-1)}{p_1 p_2 \cdots p_z}}$$

ciascuno dei quali è invariante massimo nel precedente e coi rispettivi fattori di composizione

$$p_1 \; p_2 \cdots \cdots p_z$$

L' ultimo gruppo è evidentemente il gruppo ciclico T_p col fattore di composizione p. Dunque:

Il gruppo metaciclico è un gruppo risolubile; i suoi fattori di composizione sono i fattori primi di $p-1$ e p stesso.

Dalle ricerche del § 9H risulta poi che gli unici gruppi transitivi risolubili di p lettere sono il gruppo metaciclico ed i suoi sottogruppi.

§ 38 Gruppo lineare totale sopra $p+1$ indici.

Indugiamo ora a studiare una classe di gruppi sopra $p+1$ lettere (p numero primo), che hanno una grandissima importanza nella teoria della risoluzione delle equazioni algebriche e si presentano

Altri esempi di gruppi semplici.-

Consideriamo $p+1$ simboli

$$x_\infty \; x_0 \; x_1 \; x_2 \; \ldots \; x_{p-1}$$

caratterizzati dai $p+1$ indici

$$(a) \qquad \infty, 0, 1, 2, \ldots\ldots p-1 \; ;$$

la formula

$$(1) \qquad \nu' \equiv \frac{\alpha\nu+\beta}{\gamma\nu+\delta} \pmod p \qquad (*),$$

dove $\alpha, \beta, \gamma, \delta$ sono numeri interi qualunque tali però che

$$\alpha\delta - \beta\gamma \not\equiv 0 \pmod p$$

dà una effettiva sostituzione sui $p+1$ indici (a) poichè, come subito si vede, la (1) trasporta indici diversi in indici diversi. Notiamo che i numeri $\alpha\beta\gamma\delta$ non sono presi in modo assoluto ma solo rispetto al modulo p. La (1) non rimane alterata scrivendola

$$\nu' \equiv \frac{\alpha\nu+\beta}{\gamma\nu+\delta} \pmod p$$

(*) Ricordiamo che nella teoria dei numeri col simbolo frazionario $\frac{a}{b} \pmod p$ s'intende il numero intero x che soddisfa la congruenza

$$bx \equiv a \pmod p$$

che esiste ed è unico se $b \not\equiv 0 \pmod p$. Per $b \equiv 0$ si prenderà $x = \infty$. Queste convenzioni abbreviano alcune enunciazioni

con r qualunque purché $\not\equiv 0 \pmod p$. Viceversa due sostituzioni (1) sono identiche solo quando i nuovi valori di $\alpha, \beta, \gamma, \delta$ sono proporzionali (mod p) agli antichi.

Il determinante $\Delta = \alpha\delta - \beta\gamma$ della sostituzione si cangia allora in $r^2\Delta$ e rimane quindi residuo o non residuo quadratico (mod p) a seconda del carattere di Δ. Se quindi Δ è residuo potremo rendere

$$r^2\Delta \equiv 1 \pmod p$$

e se Δ è non residuo

$$r^2\Delta \equiv q \pmod p$$

essendo q un non residuo fisso.

La totalità delle sostituzioni (1) è identica quindi a quella che si ottiene facendo percorrere ad $\alpha, \beta, \gamma, \delta$ tutti i numeri che soddisfano alla congruenza

$$(2) \qquad \alpha\delta - \beta\gamma \equiv 1 \pmod p$$

o all'altra

$$(3) \qquad \alpha\delta - \beta\gamma \equiv q \pmod p$$

Due sostituzioni (1) in cui $\alpha, \beta, \gamma, \delta$ soddisfino alla (2) o alla (3) saranno identiche solo quando i nuovi valori $\alpha', \beta', \gamma', \delta'$ soddisfino alle congruenze

$$\alpha' \equiv -\alpha\,, \quad \beta' \equiv -\beta\,, \quad \gamma' \equiv -\gamma\,, \quad \delta' \equiv -\delta \pmod p$$

---

leggi della frazione ordinaria.

queste sostituzioni (1) formano un gruppo poiché da

$$v' \equiv \frac{\alpha v + \beta}{\gamma v + \delta}, \qquad v'' \equiv \frac{\alpha' v' + \beta'}{\gamma' v' + \delta'}$$

viene

$$v'' \equiv \frac{(\alpha'\alpha + \beta'\gamma) v + (\alpha'\beta + \beta'\delta)}{(\gamma'\alpha + \delta'\gamma) v + (\gamma'\beta + \delta'\delta)}$$

Indicando simbolicamente la sostituzione (1) con $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$ vediamo che due sostituzioni del gruppo (1) si compongono secondo la legge

$$\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix} \begin{pmatrix} \alpha', \beta' \\ \gamma', \delta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + \gamma\beta', & \beta\alpha' + \delta\beta' \\ \alpha\gamma' + \gamma\delta', & \beta\gamma' + \delta\delta' \end{pmatrix}$$

onde si vede che il determinante della sostituzione composta è eguale al prodotto dei determinanti delle componenti.

Il gruppo delle sostituzioni (1) si dirà il gruppo lineare totale e in primo luogo dovremo valutare il suo ordine per il che basta contare quante soluzioni distinte hanno le congruenze (2) (3). Nella (2) p. es. se

$$\gamma \equiv 0 \pmod{p}$$

possiamo dare a β qualunque valore, ad α qualunque valore escluso $\alpha \equiv 0$ e ne risulta individuato δ; dunque la (2) ha

$$p(p-1) \text{ soluzioni con } \gamma \equiv 0$$

se $\gamma \not\equiv 0 \pmod{p}$ si può dare tanto ad α che a δ va-

Poi arbitrari e β ne risulta determinato, il che da

$$p^2(p-1) \text{ sostituzioni con } \gamma \not\equiv 0 \pmod p$$

La congruenza (2) ha dunque

$$p(p-1) + p^2(p-1) = p(p-1)(p+1).$$

soluzioni diverse e così dicasi della (3). E siccome due soluzioni opposte $(\alpha, \beta, \gamma, \delta)\ (-\alpha, -\beta, -\gamma, -\delta)$ danno luogo alla medesima sostituzione abbiamo il risultato:

Il gruppo lineare totale (1) contiene

$$p(p-1)(p+1) = p(p^2-1)$$

sostituzioni.—

In questo gruppo le sostituzioni che soddisfano alla congruenza (2) formano evidentemente un sottogruppo invariante di ordine $\frac{p(p^2-1)}{2}$. Questo gruppo

$$v' \equiv \frac{\alpha v + \beta}{\gamma v + \delta}, \quad \alpha\delta - \beta\gamma \equiv 1 \pmod p$$

si dirà il gruppo lineare speciale od anche il gruppo modulare perchè esso si presenta appunto nella teoria delle funzioni modulari ellittiche.—

Osserviamo ora che il gruppo lineare totale è triplicemente transitivo perchè, essendo i, k, l, tre indici qualunque, la sostituzione

$$v' \equiv \frac{l-i}{l-k} \cdot \frac{v-k}{v-i}$$

rispettivamente gli indici i, k, l rispettivamente in $\infty, 0, 1$ .. come il gruppo metaciclico, anche il gruppo lineare totale ha il minimo ordine compatibile col suo grado di transitività

§ 39.— **Periodo delle sostituzioni del gruppo lineare totale.** — Per determinare i diversi periodi che possono offrire le sostituzioni del gruppo lineare, cominciamo dal ricercare se vi sono indici che rimangono fissi per una sostituzione (1) .— Se $\underline{x}$ è un tale indice, dovremo avere:

$$x \equiv \frac{\alpha x + \beta}{\gamma x + \delta} \pmod p$$

cioè $$\gamma x^2 + (\delta - \alpha) x - \beta \equiv 0 \pmod p$$

Se per un momento escludiamo il caso $\gamma \equiv 0$ che dà le note sostituzioni del gruppo metaciclico e moltiplichiamo la precedente congruenza per 4γ essa diventa

$$(4) \qquad \{ 2\gamma x + (\delta - \alpha) \}^2 \equiv \Delta \pmod p$$

ove si è posto

$$(5) \qquad \Delta \equiv (\delta - \alpha)^2 + 4\beta\gamma \equiv (\alpha + \delta)^2 - 4\Delta$$

Ed ora distinguiamo tre casi e cioè

$$a) \qquad \Delta \equiv 0 \pmod p$$

Allora la (4) ha una sola radice e però la sostituzione

lascia fisso un solo elemento e sposta tutti gli altri p. La sostituzione dicesi allora **parabolica**

b) $\mathfrak{D} \not\equiv 0$ con $\mathfrak{D}$ residuo quadratico (mod p)

ossia $\left(\frac{\mathfrak{D}}{p}\right) = +1$

La (4) ha allora due radici distinte e la sostituzione dicesi **ellittica**; essa lascia fermi due indici e sposta gli altri $p-1$

c) $\mathfrak{D}$ non residuo (mod p) $\left(\frac{\mathfrak{D}}{p}\right) = -1$

La (4) non ha radici, la sostituzione prende il nome di **iperbolica**; essa sposta tutti i $p+1$ indici.

Nel caso escluso $\gamma \equiv 0 \pmod p$ la sostituzione (1) ha la forma intera del gruppo metaciclico

$$\mathfrak{D}' \equiv a\mathfrak{D} + b$$

ed è parabolica se $a \equiv 1$, ellittica se $a \not\equiv 1 \pmod p$ e poichè qui si ha $\mathfrak{D} = (a-1)^2$.

vediamo che anche il caso $\gamma \equiv 0$ rientra nel generale.

Determiniamo ora successivamente il periodo delle diverse specie di sostituzioni

a') **Sostituzioni paraboliche.** Se la sostituzione S in discorso lascia fermo x_i partiamo da S una sostituzione T che porti x_i in ∞ e la $T^{-1}ST$ sarà una sostituzione parabolica (perchè essa è fermo un so-

lo elemento) che lascia ferma $x\infty$ ed avrà perciò la forma $v' \equiv v + b$

Dunque: Le sostituzioni paraboliche hanno per periodo p.-

b') Sostituzioni ellittiche.- Se una sostituzione S lascia fermi due indici ve ne sarà una affine nel gruppo che lascerà fermi i due elementi $0, \infty$ ed avrà perciò la forma

$$v' \equiv a\,v$$

Dunque: Le sostituzioni ellittiche hanno per periodo un divisore di p-1.-

c') Diciamo ora che: Le sostituzioni iperboliche hanno per periodo un divisore di p+1.-

Il teorema sarà dimostrato quando si provi che ogni sostituzione iperbolica, decomposta in cicli, deve presentare tutti i cicli di un medesimo numero di lettere poichè essa sposta tutte le p+1 lettere. Supponiamo S decomposta in cicli e sia

$$S = C_1\, C_2\, C_3 \ldots\ldots;$$

indichiamo con z l'ordine di C_1 con s quello di C_2 e supponiamo, se è possibile, $z < s$.- La potenza S^z di S è differente dall'identità e lascia fermi almeno gli z ele-

menti di C_1 ciò che è impossibile se non è $\tau = 2$.-
Ma se S contiene un ciclo di secondo ordine essa è affine ad una sostituzione S_1 iperbolica col ciclo $(0\ \infty)$ ed S_1 avrà l'espressione analitica

$$v' \equiv \frac{b}{v} \pmod p$$

e però sarà a periodo 2 onde anche tutti gli altri cicli di S_1 e di S saranno di 2° ordine c. d. d.

§ 10.- **Sostituzioni generatrici del gruppo modulare.**- Come già abbiamo detto, il gruppo lineare totale contiene come sottogruppo invariante di indice 2 il gruppo modulare

$$v' \equiv \frac{\alpha v + \beta}{\gamma v + \delta} \pmod p, \quad \alpha\delta - \beta\gamma \equiv 1$$

d'ordine $\frac{p(p^2-1)}{2}$.- Per dimostrare, come faremo nel prossimo §, che il gruppo modulare appena $p > 3$ è semplice è utile osservare che l'intero gruppo modulare si può generare colle due sostituzioni elementari

$$S = \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$$

ossia

$$S)\ v' \equiv v + 1 \qquad T)\ v' \equiv -\frac{1}{v} \pmod p$$

Per dimostrarlo cominciamo dall'osservare che con S, T si compone la sostituzione $S_1 = TST = \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}$.-

Nel gruppo Γ generato da S, T esiste dunque qualunque potenza S^b di S e qualunque potenza S_1^c di S_1; ma si ha

$$S^b = \begin{pmatrix} 1, & b \\ 0, & 1 \end{pmatrix} \qquad S_1^c = \begin{pmatrix} 1, & 0 \\ c, & 1 \end{pmatrix}$$

e perciò in Γ vi è anche la sostituzione

$$S^b S_1^c = \begin{pmatrix} 1, & b \\ 0, & 1 \end{pmatrix}\begin{pmatrix} 1, & 0 \\ c, & 1 \end{pmatrix} = \begin{pmatrix} 1+bc, & b \\ c, & 1 \end{pmatrix}$$

Facendo $bc \equiv -1 \pmod p$ abbiamo dunque in Γ la sostituzione

$$\begin{pmatrix} 1, & b \\ -b^{-1}, & 0 \end{pmatrix}$$

con b qualunque e però anche

$$\begin{pmatrix} 1, & b \\ -b^{-1}, & 0 \end{pmatrix}\begin{pmatrix} 1, & b \\ 0, & 1 \end{pmatrix} = \begin{pmatrix} 0, & b \\ -b^{-1}, & 0 \end{pmatrix}$$

come pure

$$\begin{pmatrix} 0, & b \\ -b^{-1}, & 0 \end{pmatrix}\begin{pmatrix} 0, & -1 \\ +1, & 0 \end{pmatrix} = \begin{pmatrix} b^{-1}, & 0 \\ 0, & b \end{pmatrix}$$

Ora supponiamo dapprima che nella sostituzione $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ sia $\alpha \equiv 0$ o $\beta \equiv 0 \pmod p$. Nel primo caso componendo la $\begin{pmatrix} 0, & \beta \\ -\beta^{-1}, & \delta \end{pmatrix}$ con $\begin{pmatrix} 1, & \delta\beta \\ 0, & 1 \end{pmatrix}$ che è in Γ, si ha

$$\begin{pmatrix} 1, & \delta\beta \\ 0, & 1 \end{pmatrix}\begin{pmatrix} 0, & \beta \\ -\beta^{-1}, & \delta \end{pmatrix} = \begin{pmatrix} 0, & \beta \\ -\beta^{-1}, & 0 \end{pmatrix} ;$$

e quindi $\begin{pmatrix} 0, & \beta \\ -\beta^{-1}, & \delta \end{pmatrix} = \begin{pmatrix} 1, & -\beta\delta \\ 0, & 1 \end{pmatrix}\begin{pmatrix} 0, & \beta \\ -\beta^{-1}, & 0 \end{pmatrix}$ è in Γ.

Similmente si ha

$$\begin{pmatrix} 1, & 0 \\ -\alpha\gamma, & 1 \end{pmatrix}\begin{pmatrix} \alpha, & 0 \\ \gamma, & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} \alpha, & 0 \\ 0, & \alpha^{-1} \end{pmatrix}$$

e però anche tutte le sostituzioni $\begin{pmatrix} \alpha, & 0 \\ \gamma, & \delta \end{pmatrix}$ ove α o γ sia $\equiv 0 \pmod p$ trovansi in T. Siano ora

$$\alpha \not\equiv 0 \qquad \beta \not\equiv 0 \pmod p ;$$

Avendosi $\begin{pmatrix} 1, & m \\ 0, & 1 \end{pmatrix}\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \begin{pmatrix} \alpha & \beta + m\alpha \\ \gamma & \beta + m\gamma \end{pmatrix}$

basta determinare $\underline{m}$ dalla congruenza

$$m\alpha \equiv -\beta \pmod p$$

per avere una sostituzione con $\beta \equiv 0$, che si compone quindi con S, T c. a. d.–

Delle due sostituzioni $\begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}$, $\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$ generatrici del gruppo modulare la prima è parabolica e la seconda è ellittica od iperbolica secondo che $\left(\frac{-1}{p}\right) = \pm 1$ cioè secondo che $p \equiv 1$ ovvero $p \equiv 3 \pmod 4$.– Si vede inoltre che S, T sono ambedue sostituzioni pari. Per la prima che è parabolica, quindi a periodo p, la cosa è evidente; per la seconda si osservi che se $p \equiv 1 \pmod 4$ essa lascia ferme due lettere e contiene le rimanenti in $\frac{p-1}{2}$ cicli del 2° ordine, mentre se $p \equiv 3 \pmod 4$ la T consta di $\frac{p+1}{2}$ trasposizioni.–

Il gruppo modulare contiene dunque soltanto sosti-

tuzioni pari laddove il gruppo lineare totale ne contiene anche delle dispari come p.es. la

$$\begin{pmatrix} g, & 0 \\ 0, & 1 \end{pmatrix},$$

essendo g radice primitiva (mod p).. Come sostituzioni generatrici del gruppo lineare totale potremo assumere le tre

$$S = \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad U = \begin{pmatrix} g, & 0 \\ 0, & 1 \end{pmatrix}$$

§ 41.. Il gruppo modulare per $p > 3$ è semplice.. Dimostriamo ora l'importante teorema: **Il gruppo modulare Γ di $\frac{p(p^2-1)}{2}$ sostituzioni sopra $p+1$ lettere è semplice appena $p > 3$..** Se $p \equiv 3$, il gruppo modulare non è altro che il gruppo alterno sopra le lettere ed è risolubile..

Supponiamo che in Γ esista un sottogruppo invariante H.. Essendo Γ doppiamente transitivo sarà H almeno una volta transitivo perchè se

$$(x_i \; x_k \ldots\ldots)$$

è un ciclo di una sua sostituzione U e se V è una sostituzione di Γ che porta rispettivamente $x_i x_k$

in $x_0 x_1$ la $V^{-1} U V$ apparterrà ad H e conterrà il ci
clo $(x_0 x_1 \ldots\ldots)$
che porta x_0 in una lettera qualunque x_1, onde
H è transitivo.- Il suo ordine deve essere perciò divisibi
le per $p+1$.-
Ciò premesso dimostriamo:
1°) H non può contenere sostituzioni paraboli
che.- Sia U una sostituzione parabolica in H che
lasci ferma x_i; se la trasformiamo con una Λ di
Γ che porti x_i in x_∞ otterremo in H la sostituzio
ne $\Lambda^{-1} U \Lambda$ che sarà parabolica e lascierà ferma x_∞
e avrà perciò la forma

$$U_1 = \begin{pmatrix} 1, & \beta \\ 0, & 1 \end{pmatrix} \qquad \beta \not\equiv 0 \pmod p$$

In H sono contenute tutte le potenze di U_1 e pe
ò anche la sostituzione elementare

$$S = \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}$$

di Γ e qualunque sua potenza.- Ma essendo H in
variante in Γ, se contiene una sostituzione

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

contiene anche le sue trasformate per S e per T cioè

$$\mathcal{T}^{-1}\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}\mathcal{T} = \begin{pmatrix}-\delta, & \gamma\\ \beta, & -\alpha\end{pmatrix}$$

$$\mathcal{S}^{-1}\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}\mathcal{S} = \begin{pmatrix}\alpha+\gamma, & (\beta+\delta)-(\alpha+\gamma)\\ \gamma & \delta-\gamma\end{pmatrix}$$

Contenendo $\begin{pmatrix}1, & \gamma\\ 0, & 1\end{pmatrix}$ con γ qualunque, H contiene anche

$$\mathcal{T}^{-1}\begin{pmatrix}1, & \gamma\\ 0, & 1\end{pmatrix}\mathcal{T} = \begin{pmatrix}1, & 0\\ -\gamma, & 1\end{pmatrix}$$

e però anche $\begin{pmatrix}1, & 0\\ -1, & 1\end{pmatrix}\begin{pmatrix}1, & 1\\ 0, & 1\end{pmatrix} = \begin{pmatrix}0, & 1\\ -1, & 1\end{pmatrix}$

quindi il prodotto $\begin{pmatrix}1, & 1\\ 0, & 1\end{pmatrix}\begin{pmatrix}0, & 1\\ -1, & 1\end{pmatrix} = \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix} = \mathcal{T}$.-

Ne segue che H contenendo le due sostituzioni $\mathcal{S}, \mathcal{T}$ generatrici di Γ coincide con Γ c.d.d.

2°) H non può contenere sostituzioni ellittiche.- Se H contiene una sostituzione ellittica, ne conterrà una affine che lascia fermi gli indici $0, \infty$ e perciò della forma

$$\mathcal{U} = \begin{pmatrix}\alpha, & 0\\ 0, & \alpha^{-1}\end{pmatrix}$$

In H avremo quindi anche la

$$\mathcal{U}_1 = \mathcal{S}^{-1}\mathcal{U}\mathcal{S} = \begin{pmatrix}\alpha, & \alpha^{-1}-\alpha\\ 0, & \alpha^{-1}\end{pmatrix}$$

e però anche

$$\mathcal{U}_1\mathcal{U}^{-1} = \begin{pmatrix}\alpha, & \alpha^{-1}-\alpha\\ 0, & \alpha^{-1}\end{pmatrix}\begin{pmatrix}\alpha^{-1} & 0\\ 0 & \alpha\end{pmatrix} = \begin{pmatrix}1, & \alpha^{-1}(\alpha^{-1}-\alpha)\\ 0, & 1\end{pmatrix}$$

che è parabolica. Dunque H coincide con T.

3°) Resta dunque da vedersi se con sostituzioni tutte iperboliche H di T. L'ordine di H essendo divisibile per $p+1$ quindi per 2, H conterrà una sostituzione U iperbolica a periodo 2. Se $(x_1 x_2)$ è un ciclo di U, trasformando U colla sostituzione $v' \equiv v - a \pmod p$ di T avremo in H una sostituzione della trasposizione $(0\ \infty)$ e perciò della forma

$$U_1 = \begin{pmatrix} 0, & \beta \\ -\beta^{-1}, & 0 \end{pmatrix}$$

Perchè la U_1 sia iperbolica deve aversi

$$\left(\frac{-1}{p}\right) = -1$$

quindi $p \equiv 3 \pmod 4$. Anche la trasformata U_2 di U_1 per mezzo di τ sarebbe in H cioè

$$U_2 = \begin{pmatrix} 0, & -\beta^{-1} \\ \beta, & 0 \end{pmatrix}$$

onde anche

$$U_1 U_2 = \begin{pmatrix} \beta^{-2}, & 0 \\ 0, & \beta^2 \end{pmatrix}$$

che è ellittica se non è l'identità. Dunque

$$\beta^4 \equiv 1 \pmod p$$

onde a causa di $p \equiv 3 \pmod 4$ si ha

$$\beta \equiv \pm 1 \pmod 4$$

e perciò U_1 coincide con τ che trovasi dunque in H.

In H saremo quindi anche

$$\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}^{-1} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} \begin{pmatrix} a, & b \\ c, & d \end{pmatrix} = \begin{pmatrix} -(ac+bd), & a^2+b^2 \\ -(c^2+d^2), & ac+bd \end{pmatrix}$$

con a, b, c, d qualunque purchè

$$ad - bc \equiv 1$$

assumiamo c, d ad arbitrio e determiniamo a, b dalle congruenze

$$\begin{aligned} d \cdot a - c \cdot b &\equiv 1 \\ c \cdot a + d \cdot b &\equiv 0 \end{aligned} \pmod{p}$$

il cui determinante $c^2 + d^2$ è certo $\not\equiv 0 \pmod{p}$.—
In H esiste dunque la sostituzione

$$\begin{pmatrix} 0 & -(c^2+d^2)^{-1} \\ c^2+d^2 & 0 \end{pmatrix}$$

e per quanto si è visto sopra dobbiamo quindi avere

$$c^2 + d^2 \equiv \pm 1 \pmod{p}$$

e facendo $c = d = 1$ risulta necessariamente $p = 2$.
Così il nostro Teorema è completamente dimostrato.—

Osservazione. — I gruppi modulari per $p = 5$, $p = 7$ sono gruppi semplici di

$$60 \text{ e } 168$$

sostituzioni rispettivamente sopra 6 e sopra 8 elementi.— Il primo [illegible], come abbiamo visto al

§ 29 è identicamente isomorfo col gruppo alterno su 5 lettere. Il secondo è il gruppo semplice di cui al § 28 abbiamo già annunciata l'esistenza.

§ 31. **Gruppi di sostituzioni lineari sopra una variabile.** Le sostituzioni lineari sopra una variabile x:

$$(1) \qquad x' = \frac{\alpha x + \beta}{\gamma x + \delta}$$

dove i coefficienti $\alpha, \beta, \gamma, \delta$ sono costanti qualunque che non rendano però zero il determinante della sostituzione $\alpha\delta - \beta\gamma$ (*), sono operazioni suscettibili di composizione. Se indichiamo simbolicamente con $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ la sostituzione (1) l'effetto di due successive sostituzioni lineari $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$ è una terza sostituzione lineare (cf § 30) (**)

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + \gamma\beta', & \beta\alpha' + \delta\beta' \\ \alpha\gamma' + \gamma\delta', & \beta\gamma' + \delta\delta' \end{pmatrix}$$

(*) Se $\alpha\delta - \beta\gamma = 0$ la (1) non rappresenta più una sostituzione su x, il 2° membro essendo indipendente da x.

(**) Si può anche verificare con questa formula di composizione che componendo più sostituzioni lineari vale la legge associativa.

Possiamo quindi considerare gruppi finiti od infiniti di sostituzioni lineari (1) e noi qui ci proponiamo di studiare i gruppi finiti di tali sostituzioni e di costruire tutti i possibili tipi di tali gruppi. (*). Osserviamo ora che nella (1) si cangia linearmente la variabile z in

$$t = \begin{pmatrix} a, b \\ c, d \end{pmatrix} z = \frac{az+b}{cz+d}$$

e colla medesima sostituzione la trasformata z' in

$$t' = \begin{pmatrix} a, b \\ c, d \end{pmatrix} z'$$

sarà t legata linearmente a t' dalla sostituzione trasformata di $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$

$$\begin{pmatrix} a & b \\ c, d \end{pmatrix}^{-1} \begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix} \begin{pmatrix} a, b \\ c, d \end{pmatrix}$$

Se consideriamo una totalità di sostituzioni (1) formanti un gruppo G, cangiando linearmente la va-

---

(*) Un esempio ben noto di tali gruppi c'è fornito dalle 6 espressioni diverse del rapporto anarmonico di quattro elementi di una forma geometrica di 1ª specie, ottenute col cangiare l'ordine degli elementi stessi e

riabile avremo un nuovo gruppo

$$G' = \begin{pmatrix} a, & b \\ c, & d \end{pmatrix}^{-1} G \begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$$

che riguardiamo come appartenente al medesimo tipo di G.-

La sostituzione (1) lascia fissi due valori della variabile complessa z, cioè le radici della equazione (2) $\gamma z^2 + (\delta - \alpha) z - \beta = 0$

Chiameremo questi due valori di z i **poli** della sostituzione (1) ed anzi tutto dimostreremo:

Ogni sostituzione lineare (1) che fa parte di un gruppo finito G ha necessariamente i suoi poli distinti.-

Ciò si dimostra facilmente osservando che una tale sostituzione S deve avere un periodo finito. Ora se S avesse i suoi due poli coincidenti avremmo

(3) $\qquad (\delta - \alpha)^2 - 4\beta\gamma = 0$

Supponiamo dapprima $\beta \neq 0$ e $\gamma = 0$ onde $\alpha = \delta$ e

---

cioè il gruppo $G_6 = \left(z,\ 1-z,\ \frac{1}{z},\ \frac{1}{1-z},\ \frac{z}{z-1},\ \frac{z-1}{z} \right)$ che nella classificazione successiva apparirà come gruppo diedrale (per $n = 3$)

senza alterare la generalità potremo fare $\alpha = \delta = 1$, onde

$$S = \begin{pmatrix} 1, & \beta \\ 0, & 1 \end{pmatrix} \quad \text{ovvero} \quad S = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$$

Essendo m un numero intero avremo nel primo caso

$$S^m = \begin{pmatrix} 1, & m\beta \\ 0, & 1 \end{pmatrix} \text{ e nel secondo } S^m = \begin{pmatrix} 1 & 0 \\ m\gamma & 1 \end{pmatrix}$$

e non potrà mai essere $S^m = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$. - Se poi $\gamma \neq 0$ basterà sostituire ad S una sua trasformata

$$T^{-1} S T$$

con $\gamma = 0$, per il che basta assumere per T una sostituzione che trasporti il polo di S in $z = \infty$. -

§ 43. - **Poli delle sostituzioni di un gruppo finito.** - Supponiamo di avere un gruppo finito G d'ordine m di sostituzioni lineari sulla variabile z, siano

$$\psi_i(z) = \frac{a_i z + b_i}{c_i z + d_i} \qquad (i = 1, 2, 3 \ldots m)$$

fra le quali figurerà naturalmente l'identità, poniamo sia

$$\begin{pmatrix} a_1, & b_1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$$

cioè $\psi_1(z) = z$. Ciascuna delle $m-1$ rimanenti ha due

poli distinti, onde il numero totale dei poli delle sostituzioni di G sarà

$$N = 2(m-1),$$

quando naturalmente si conti ogni polo tante volte quante sono le sostituzioni del gruppo esclusa l'identità per le quali è punto fisso. - Sia $z = k$ un polo comune a ν sostituzioni di G (l'identità compresa) e siano p. es.

$$(4) \qquad \psi_1(z)\,\psi_2(z)\,\dots\dots\,\psi_\nu(z)$$

queste ν sostituzioni talchè

$$\psi_1(k) = k\,,\quad \psi_2(k) = k\,\dots\dots\,\psi_\nu(k) = k.$$

In primo luogo vediamo che le ν sostituzioni (4) aventi a comune il polo k formano in G un sottogruppo, poichè da

$$k = \psi_i(k)\,,\quad k = \psi_j(k)$$

segue $$k = \psi_i(\psi_j(k)).$$

Di più diciamo: — **Il sottogruppo T formato dalle ν sostituzioni (4) che hanno a comune un polo k è un gruppo ciclico** cioè è formato dalle potenze di una delle (4) a periodo ν. —

Cangiando linearmente la variabile z possiamo

trasportare il polo k in $z = \infty$ e le ν sostituzioni acquisteranno la forma

$$\psi_1(z) = z\,, \quad \psi_i(z) = \varepsilon_i z + c_i \qquad (i = 2, 3, \ldots \nu)$$

Ripetendo ν volte una qualunque di queste ψ, deve ottenersi l'identità e però si ha

$$\varepsilon_i^{\nu} = 1$$

cioè $\varepsilon_1 = 1\,,\ \varepsilon_2\,,\ \varepsilon_3 \ldots\ldots\ldots \varepsilon_\nu$ sono tutte radici ν^{me} dell'unità, onde se proviamo che sono tutte diverse fra loro le ν ε saranno potenze di una medesima radice primitiva. Intanto, cangiando z in $z +$ costante, possiamo fare una delle c p. es. $c_2 = 0$ (*) e dico allora che ogni altra c p. es. c_3 risulterà nulla. Infatti essendo $\psi_2(z) = \varepsilon_2 z\,,\ \psi_3(z) = \varepsilon_3 z + c_3$ sarà

$$\psi_i\left[\psi_3(z)\right] = \varepsilon_2\varepsilon_3 z + \varepsilon_2 c_3\,,\quad \psi_3\left[\psi_2(z)\right] = \varepsilon_2\varepsilon_3 z + c_3$$

quindi nel gruppo avremmo anche la sostituzione

$$z' = z + \frac{c_3(\varepsilon_2 - 1)}{\varepsilon_2\,\varepsilon_3}$$

che non ha periodo finito se non è $c_3 = 0$. — Dopo ciò

(*) Basta cangiare z in $z + \frac{c_2}{1-\varepsilon_2}$.—

è chiaro che tutte le ε sono diverse fra loro c.d.d.

Così il teorema è dimostrato e di più vediamo che: **tutte le sostituzioni del sottogruppo ciclico T hanno non solo il primo ma anche il secondo polo a comune.** Ora se k è un polo e ψ una qualunque sostituzione del gruppo sarà anche $k' = \psi(k)$ un polo e precisamente sarà polo comune a tutte le sostituzioni trasformate per mezzo di ψ delle sostituzioni che lasciano fermo k.

Due tali poli si diranno equivalenti ed è chiaro che due poli equivalenti ad un terzo sono equivalenti fra loro onde potremo ripartire i $2(m-1)$ poli in classi, ponendo nella medesima classe quelli che sono fra loro equivalenti.

Essendo k un polo d'ordine ν cioè comune a $\nu-1$ sostituzioni di G (oltre l'identità) è facile subito che nella classe di k vi sono precisamente $\frac{m}{\nu}$ poli distinti tutti dell'ordine ν (*).

(*) Ed infatti vi sono in G ν sostituzioni coniugate, quelle del sottogruppo T_1 che lasciano fermo k onde data $\underline{m}$ sostituzioni di G k è portato in $\frac{m}{\nu}$ poli distinti.

Se supponiamo dunque che i poli si ripartiscano in r classi con poli delle rispettive molteplicità

$$\nu_1 \quad \nu_2 \quad \ldots\ldots \quad \nu_r$$

avremo nella classe con poli di multiplicità ν_i precisamente $\frac{m}{\nu_i}(\nu_i - 1)$ poli. Dovremo quindi avere

$$\sum_{i=1}^{i=r} \frac{m}{\nu_i}(\nu_i - 1) = 2m - 2$$

ovvero

$$(A) \qquad \sum_{i=1}^{i=r} \left(1 - \frac{1}{\nu_i}\right) = 2 - \frac{2}{m} .$$

§ 44. — Enumerazione dei possibili tipi.

Ora discutendo l'equazione d'analisi indeterminata (A) nella quale ciascun numero ν_i deve essere un intero ≥ 2 è facile enumerare i possibili tipi di gruppi di sostituzioni lineari:

Intanto osserviamo che sarà necessariamente $1 < r \leq 3$ perchè se $r = 1$ il 1° membro della (A) sarebbe < 1 laddove il secondo è certo > 1 a causa di $m \leq 2$. Nè può essere $r \geq 4$ perchè allora il 1° membro della (A), contando almeno di 4 termini ciascuno $\geq \frac{1}{2}$, sarebbe ≥ 2 mentre il 2° invece è < 2. — Abbiamo dunque necessariamente $r = 2$ o $r = 3$ —

1° caso.— $r = 2$. Avremo

$$\frac{1}{\nu_1} + \frac{1}{\nu_2} = \frac{2}{m} ;$$

ma poichè deve essere

$$\nu_1 \leq m \qquad \nu_2 \leq m$$

sarà necessariamente

$$\nu_1 = m \qquad \nu_2 = m$$

Si ha dunque una prima soluzione della (A)

I) m qualunque $\nu_1 = \nu_2 = m$

2° caso $r = 3$.— Dovendo essere

$$(B) \qquad \frac{1}{\nu_1} + \frac{1}{\nu_2} + \frac{1}{\nu_3} = 1 + \frac{2}{m}$$

uno almeno dei numeri $\nu_1\ \nu_2\ \nu_3$ sarà $= 2$ perchè altrimenti il primo membro della (B) sarebbe ≤ 1

Facciamo dunque $\nu_1 = 2$ e rimarrà

$$(C) \qquad \frac{1}{\nu_2} + \frac{1}{\nu_3} = \frac{1}{2} + \frac{2}{m} ;$$

Se anche uno dei due numeri ν_2, ν_3 è $= 2$, per esempio $\nu_2 = 2$, resta $\nu_3 = \frac{m}{2}$ e si ottiene una seconda soluzione della (A):

II) $m = 2n$; $\nu_1 = 2$, $\nu_2 = 2$, $\nu_3 = n$ (n qualunque)

Ora siano $\nu_2 > 2$, $\nu_3 > 2$; allora uno dei due sarà $= 3$ perchè se fosse $\nu_2 > 3$, $\nu_3 > 3$ il primo membro della (C) sarebbe $\leq \frac{1}{2}$.— Poniamo dunque che sia $\nu_2 = 3$ e rimarrà $\frac{1}{\nu_3} = \frac{1}{6} + \frac{2}{m}$ onde sarà ancora $\nu_3 < 0$

e facendo successivamente

$$\nu_3 = 3, 4, 5$$

troviamo le nuove soluzioni

(III)	$m = 12$	$\nu_1 = 2$	$\nu_2 = 3$	$\nu_3 = 3$
(IV)	$m = 24$	$\nu_1 = 2$	$\nu_2 = 3$	$\nu_3 = 4$
(V)	$m = 60$	$\nu_1 = 2$	$\nu_2 = 3$	$\nu_3 = 5$

Dimostreremo che alle possibili soluzioni della nostra equazione d'analisi indeterminata (A), così enumerate corrispondono effettivamente altrettanti tipi di gruppi di sostituzioni lineari, ad ogni soluzione corrispondendo un unico tipo. Questi gruppi, per una ragione che vedremo in seguito, portano i nomi seguenti

Tipo I) gruppi ciclici (o della piramide regolare)
" II) gruppi del diedro (o della doppia piramide)
" III) gruppo del tetraedro
" IV) gruppo dell'ottaedro (o cubo)
" V) gruppo dell'icosaedro (o dodecaedro)

§ 45. — **Gruppi ciclici e diedrali.** — Procediamo alla effettiva costruzione dei gruppi dei primi due tipi. — Un gruppo G_n del primo tipo d'ordine n, ci

sendo $\nu_1 = \nu_2 = n$, esiste una sostituzione S a periodo n e il gruppo G_n è il gruppo ciclico

$$G_n = (1, S, S^2, S^3, \ldots S^{n-1})$$

Alla sostituzione S, cangiando linearmente la variabile, si può dare la forma

$$z' = \varepsilon z$$

essendo ε una radice primitiva n^{ma} dell'unità (§ 42).

Dunque: **Un gruppo del primo tipo è ciclico e si può rappresentare analiticamente così:**

$$\alpha) \quad z' = z, \ \varepsilon z, \ \varepsilon^2 z, \ldots \varepsilon^{n-1} z \qquad \left(\varepsilon = e^{\frac{2\pi i}{n}}\right)$$

Consideriamo ora un gruppo G_m del 2° tipo con

$$m = 2n \qquad \nu_1 = \nu_2 = 2, \quad \nu_3 = n$$

A causa di $\nu_3 = n$ esso possiede un sottogruppo ciclico Γ_n d'ordine n cui possiamo dare la forma α).

Sia ora T una sostituzione a periodo 2 del gruppo; avendosi

$$G = [\Gamma, T\Gamma]$$

come anche

$$G = (\Gamma, \Gamma T)$$

avremo necessariamente

$$ST = TS^r$$

per un conveniente valore di r cioè $T^{-1}ST = S^r$.

Le supponiamo che

$$z' = \frac{\alpha z + \beta}{\gamma z + \delta}$$

sia l'espressione analitica di T, dovremo quindi avere identicamente

$$\frac{\alpha \varepsilon z + \beta}{\gamma \varepsilon z + \delta} = \varepsilon^z \frac{\alpha z + \beta}{\gamma z + \delta}$$

da cui segue subito

$$\alpha = 0 \qquad \delta = 0$$

ovvero $\qquad \beta = 0 \qquad \gamma = 0$

Il secondo caso è da escludersi perchè allora la T sarebbe come la S una sostituzione moltiplicativa $z' = az$ e conseguentemente G_m sarebbe un gruppo ciclico, cioè del primo tipo.-

La T avrà dunque la forma

$$z' = \frac{k}{z}$$

con k costante. Mutando z in $\underline{az}$ si può dare a k un valore fisso qualunque p. es. $k = -1$ e si ottiene così come forma normale dei gruppi del secondo tipo: Gruppi del diedro

$$b) \quad z' = \varepsilon^\nu z, \quad z' = -\frac{\varepsilon^\nu}{z} \quad \begin{cases} \varepsilon = e^{\frac{2\pi i}{n}} \\ \nu = 0, 1, 2, \ldots n-1 \end{cases}$$

Prima di andare effettivamente a costruire i gruppi degli altri tre tipi è utile dimostrare il seguente teore-

ma: Se un gruppo G di sostituzioni lineari sopra una variabile contiene come sottogruppo T invariante un gruppo ciclico esso appartiene al primo ovvero al secondo tipo.—

Possiamo naturalmente supporre che T non sia contenuto in un altro sottogruppo ciclico T' di G più ampio di T; altrimenti considereremmo T' in luogo di T.— Ora se n è l'ordine di T, potremo dare a questo gruppo la forma normale a).— Qualunque sostituzione di G dovendo trasformare S in una potenza di S avrà per quanto ora abbiamo visto l'una o l'altra delle due forme

$$x' = ax \quad , \quad x' = \frac{k}{x}$$

Ma il 1° caso è da escludersi perchè allora tutte le sostituzioni moltiplicative formerebbero un sottogruppo invariante T' più ampio di T.— D'altronde se $\mathcal{T}, \mathcal{T}'$ sono due sostituzioni di G fuori di T la $\mathcal{T}\mathcal{T}'$ è una sostituzione moltiplicativa e però una potenza di S.— Dunque tutte le sostituzioni di G sono nel quadro

$$G = \begin{cases} 1, S, S^2, \ldots, S^{n-1} \\ \mathcal{T}, \mathcal{T}S, \mathcal{T}S^2, \ldots \mathcal{T}S^{n-1} \end{cases}$$

e però G appartiene al secondo tipo.—

§ 46.- **Gruppo del tetraedro**.- Nel tipo III) abbiamo $m = 12$, $\nu_1 = 2$, $\nu_2 = 3$, $\nu_3 = 3$.

Il gruppo G_{12} deve contenere, pel teorema di Sylow, un numero q di sottogruppi del 3° ordine della forma

$$q = 3\tau + 1$$

e dovrà essere

$$12 = 3\delta(3\tau + 1)$$

onde

$$\tau = 0 \quad \text{o} \quad \tau = 1$$

Ma il primo caso si esclude subito perchè G avrebbe un sottogruppo invariante ciclico del 3° ordine e quindi di (§ 45) G_{12} apparterrebbe al primo o al secondo tipo.

Dunque in G_{12} esistono quattro sottogruppi

$$H_1 \; H_2 \; H_3 \; H_4$$

del 3° ordine che trasformati con tutte le sostituzioni di G danno luogo ad un gruppo T transitivo sulle 4 lettere H in isomorfismo con G.- L'isomorfismo è oloedrico perchè se n è il grado di meriedria dovrebbe essere $\frac{12}{n}$ multiplo di 4 e però

$$n = 3 \quad \text{o} \quad n = 1$$

Nel primo caso il sottogruppo Σ di G che corrisponde all'identità in T sarebbe del 3° ordine ed invariante in G ciò che è impossibile (§ 45).- Ne segue che T

è il gruppo alterno sulle quattro lettere H. Se prendiamo le tre sostituzioni di T

$$(H_1 H_2 H_3), (H_1 H_4)(H_2 H_3), (H_1 H_2)(H_3 H_4)$$

e indichiamo con S, T, T' le tre corrispondenti in G cioè che scriviamo simbolicamente

$$S \sim (H_1 H_2 H_3)$$
$$T \sim (H_1 H_4)(H_2 H_3)$$
$$T' \sim (H_1 H_2)(H_3 H_4),$$

basterà costruire le effettive espressioni di S, T, T' per conoscere tutto il gruppo G poichè colle tre corrispondenti sostituzioni sulle H si genera l'intero gruppo T.

Alla sostituzione T a periodo 2, cangiando linearmente z, potremo dare la forma (§ 45)

$$T) \qquad z' = -z$$

Ora si ha $$TT' = T'T \quad (*)$$ e però T' ha la forma moltiplicativa $z' = az$ ovvero l'altra

$$T') \qquad z' = \frac{k}{z}$$

Il 1° caso è da escludersi perchè essendo T' a periodo

(*) Per verificare le relazioni che ora scriveremo fra S, T, T' basta verificarle sulle sostituzioni corrispondenti in T, perchè l'isomorfismo di G con T è oloedrico.

2, ne seguirebbe $a=-1$ cioè $\mathcal{T}'$ coinciderebbe con $\mathcal{T}$. L'affinità mutando z in λz la $\mathcal{T}$ non si altera e alla costante k in $\mathcal{T}'$ si può dare qualsiasi valore, poniamo $k=1$, onde avremo

$$\mathcal{T}') \qquad z' = \frac{1}{z}$$

Se poniamo $\mathcal{T}'' = \mathcal{T}\mathcal{T}' = \mathcal{T}'\mathcal{T} \sim (H_1 H_3)(H_2 H_4)$

avremo per $\mathcal{T}''$ la forma

$$\mathcal{T}'') \qquad z' = -\frac{1}{z}$$

Sia ora

$$z' = \frac{\alpha z + \beta}{\gamma z + \delta}$$

la forma di $\mathcal{S}$. Osservando che si ha

$$\mathcal{T}\mathcal{S} = \mathcal{S}\mathcal{T}'' \,, \quad \mathcal{T}'\mathcal{S} = \mathcal{S}\mathcal{T}$$

ne deduciamo l'identità

$$\frac{\alpha z - \beta}{\gamma z - \delta} = -\frac{\gamma z + \delta}{\alpha z + \beta} \,, \qquad \frac{\alpha + \beta z}{\gamma + \delta z} = -\frac{\alpha z + \beta}{\gamma z + \delta}$$

e però

$$\alpha^2 + \gamma^2 = 0 \qquad \alpha\delta + \beta\gamma = 0$$

$$\beta^2 + \delta^2 = 0 \qquad \beta\delta + \alpha\gamma = 0$$

di qui segue $\beta = \pm\alpha$, $\gamma = i^\varepsilon \alpha$, $\delta = \mp i^\varepsilon \alpha$ $(i = \sqrt{-1})$, dove ε ha il valore 1 o 3; la $\mathcal{S}$ avrà dunque una delle quattro forme

$$i\,\frac{z+1}{z-1} \,, \quad i\,\frac{z-1}{z+1} \,, \quad -i\,\frac{z+1}{z-1} \,, \quad -i\,\frac{z-1}{z+1}$$

e siccome una qualunque di queste quattro sostituzio-

ni, combinata con T, T', T'', da le altre, vediamo che G le contiene tutte. Per il gruppo G da costruirsi abbiamo così ottenuta la forma normale

Gruppo del tetraedro c)

$$z' = \pm z \ , \pm\frac{1}{z} \ , \pm i\,\frac{z+1}{z-1} \ , \pm i\,\frac{z-1}{z+1} \ , \pm\frac{z+i}{z-i} \ , \pm\frac{z-i}{z+i} \ .$$

Si verifica subito che queste 12 sostituzioni formano in effetto un gruppo

§ 47. - Gruppo dell' ottaedro. - Un gruppo G del quarto tipo contiene 24 sostituzioni e quindi un certo numero di sottogruppi del 3° ordine H; come al § precedente, applicando il teorema di Sylow, si vede che esistono in G precisamente quattro sottogruppi

$$H_1 \ H_2 \ H_3 \ H_4$$

del 3° ordine. Il gruppo T che si ottiene sui quattro gruppi H trasformandoli colle sostituzioni di G è transitivo ed isomorfo con G. - Anche qui dimostriamo che l'isomorfismo è oloedrico. È invero il grado n (di meriedria) del sottogruppo Σ in G che corrisponde all'identità in T deve essere un divisore di 6 e quindi

$$n = 6 \quad o \quad n = 2 \quad o \quad n = 3 \quad o \quad n = 1$$

I due casi $n = 2$, $n = 3$ si escludono subito perchè Σ

... è invariante in G, sarebbe ciclico. Ma non può essere nemmeno $n=6$ perchè Σ conterrebbe un unico sottogruppo Σ_1 del 3° ordine, che sarebbe quindi invariante non solo in Σ ma anche in G. (*)

Dunque G è oloedricamente isomorfo col gruppo totale T_{24} sulle quattro lettere

$$H_1\ H_2\ H_3\ H_4\ ;$$

esso contiene quindi un gruppo G_{12} di 12 sostituzioni corrispondente al gruppo alterno, cioè un gruppo del tipo III che potremo già supporre ridotto alla forma normale c) del § precedente. Per determinare completamente G_{24} basterà quindi costruire una sostituzione di G_{24} fuori di G_{12}, p. es. della

$$U \sim (H_1\ H_2\ H_4\ H_3)$$

Essendo U permutabile con $T \sim (H_1 H_4)(H_2 H_3)$ avrà la forma moltiplicativa

$$x' = ax$$

ovvero l'altra $x' = \frac{k}{x}$; ma quest'ultima si esclude perchè sarebbe a periodo 2 mentre U è a periodo 4. —

(*) È infatti qualunque sostituzione g di G trasforma Σ_1 in $g^{-1}\Sigma_1 g$ che è contenuta in $g^{-1}\Sigma g = \Sigma$ e però $g^{-1}\Sigma_1 g = \Sigma_1$. —

Ora dovendo essere $a^4 = 1$ sarà

$$z' = \pm iz$$

la forma di H. - Quale dei due segni si prenda è indifferente perchè l'una delle due sostituzioni nasce dall'altra combinata con T.-

Abbiamo dunque per la forma normale dei gruppi del IV° tipo:

gruppo dell'ottaedro

d) $z' = i^\varepsilon z,\ \frac{i^\varepsilon}{z},\ i^\varepsilon \frac{z+1}{z-1},\ i^\varepsilon \frac{z-1}{z+1},\ i^\varepsilon \frac{z+1}{z-1},\ i^\varepsilon \frac{z-1}{z+1}$ $(\varepsilon = 0, 1, 2, 3.)$

Queste 24 sostituzioni formano in effetto un gruppo.-

§ 48.- **Gruppo dell'icosaedro**.- Per costruire i gruppi del V° tipo cominciamo dal dimostrare: **Un gruppo G_{60} del V° tipo è un gruppo semplice**.- Esso non può intanto contenere come sottogruppo invariante un gruppo ciclico (§ 45) e neppure un sottogruppo diedrale G_{2n} se pure escludiamo pel momento il caso $n = 2$, perchè un tale gruppo G_{2n} contiene un solo sottogruppo ciclico d'ordine n T_n che sarebbe dunque esso stesso invariante in G_{60}.- Se T_m è un sottogruppo invariante di G_{60} e non è diedrale con $m = 4$ sarà dun-

ne necessariamente $m = 12$

poichè unicamente per questo divisore di 60 si ha l'ordine di un gruppo non appartenente al 1° o 2° tipo.- Dunque si avrebbe in $\mathcal{G}_{60}$ un sottogruppo invariante $\mathcal{G}_{12}$ tetraedrale ovvero un sottogruppo $\mathcal{G}_4$ diedrale cui potremo dare la forma

$\mathcal{G}_4$) $\quad x' = x \;,\; x' = -x \;,\; x' = \frac{1}{x} \;,\; x' = -\frac{1}{x}$

Basterà considerare quest'ultimo caso giacchè se ammettiamo che $\mathcal{G}_{60}$ contenga il sottogruppo invariante $\mathcal{G}_{12}$ questo contiene poi un unico sottogruppo diedrale $\mathcal{G}_4$ che sarebbe dunque invariante in $\mathcal{G}_{12}$ ed anche in $\mathcal{G}_{60}$. Ora se S è una sostituzione a periodo 5 di $\mathcal{G}_{60}$ formando con S le tre sostituzioni di $\mathcal{G}_4$ diverse dall'identità dovranno permutarsi fra loro secondo una sostituzione a periodo 5 o restare singolarmente invariate e siccome non esiste una sostituzione su tre lettere a periodo 5 necessariamente la S sarebbe permutabile colle tre dette sostituzioni in $\mathcal{G}_4$ ciò che si vede subito essere impossibile.- Dimostrato ciò il teorema enunciato ne resulta (§ 30):

Un gruppo $\mathcal{G}_{60}$ del V° tipo è oloedricamente isomorfo col gruppo alterno su 5 lettere.-

Indicando le 5 lettere con a, b, c, d, e basterà ove costruiamo in G_{60} le sostituzioni S, T, U rispettivamente corrispondenti alle seguenti sostituzioni del gruppo alterno

$$S \sim (a\,b\,c\,d\,e)$$
$$T \sim (b\,c)(d\,e)$$
$$U \sim (b\,e)(d\,c)$$

Siccome il gruppo alterno Δ si genera colle due sostituzioni

$$(a\,b\,c\,d\,e)\ ,\ (b\,c)(d\,e) \quad (*)$$

avremo così le sostituzioni generatrici di G_{60}.-
Alla sostituzione ciclica del 5° ordine S potremo dare la forma (§ 45) $S)\ x' = \varepsilon x$ con $\varepsilon = e^{\frac{2\pi i}{5}}$.-

---

(*) Posto $A = (a\,b\,c\,d\,e)$ $B = (b\,c)(d\,e)$ $C = (b\,e)(c\,d)$ si ha invero

$$BA = (a\,b\,d)\ ,\quad C = A^2BA^3BA^2B$$

Il gruppo generato da A, B contiene adunque una sostituzione del 5° ordine A, una del 3° BA e il sottogruppo del 4° ordine

$$1,\ B,\ C,\ BC$$

onde il suo ordine è multiplo di $4 \times 5 \times 3$ è però $= 60$ c.d.d.

Sia ora la forma di $\mathcal{U}$:

$$\mathcal{U}) \qquad x' = \frac{\alpha x + \beta}{\gamma x + \delta} \; ;$$

poichè $\mathcal{U}^{-1} S \mathcal{U} = S^4$ cioè $S\mathcal{U} = \mathcal{U} S^4$, sussisterà l'identità

$$\frac{\alpha \varepsilon x + \beta}{\gamma \varepsilon x + \delta} = \varepsilon^4 \frac{\alpha x + \beta}{\gamma x + \delta}$$

da cui

$$\alpha\gamma = 0 \qquad \beta\delta = 0 \qquad \alpha\delta = 0$$

e perciò (*) $\qquad \alpha = 0 \qquad \delta = 0$

La $\mathcal{U}$ avrà dunque la forma

$$x' = \frac{k}{x}$$

e moltiplicando x per una costante potremo fissare che si abbia $k = -1$ cioè

$$\mathcal{U}) \qquad x' = -\frac{1}{x}$$

Sia ora

$$\mathcal{T}) \qquad x' = \frac{ax + b}{cx + d} \; ;$$

essendo $\mathcal{T}^2 = 1$ sarà intanto (**)

$$a + d = 0$$

e poichè $\mathcal{T}\mathcal{U} = \mathcal{U}\mathcal{T}$ avremo

$$-\frac{cx + d}{ax + b} = \frac{bx - a}{dx - c} \; ,$$

(*) Si osservi che non può essere nè $\beta = 0$ nè $\gamma = 0$ perchè altrimenti sarebbe $\alpha\delta - \beta\gamma = 0$

(**) Infatti $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}^2 = \begin{pmatrix} a^2 + bc, & b(a+d) \\ c(a+d), & a^2 + bc \end{pmatrix}$

onde $ab + cd = 0$, $a^2 + c^2 = b^2 + d^2$

e perciò $d = -a$ $\quad b = c$ (*)

Abbiamo dunque per $\mathcal{T}$

$$\mathcal{T}) \quad z' = \frac{az + b}{bz - a}$$

Facciamo ora uso dell' identità

$$\mathcal{U} = \mathcal{S}^2 \mathcal{T} \mathcal{S}^3 \mathcal{T} \mathcal{S}^2 \mathcal{T}$$

che scriviamo

$$\mathcal{U}\mathcal{T} = \mathcal{S}^2 \mathcal{T} \mathcal{S}^3 \mathcal{T} \mathcal{S}^2$$

e ne ricaviamo

$$\frac{a - bz}{az + b} = \frac{(\varepsilon^2 a^2 + \varepsilon^4 b^2) z + (1 - \varepsilon^2) ab}{(1 - \varepsilon^2) ab z + (\varepsilon^2 b^2 + a^2)}$$

da cui

$$a^2 (1 + \varepsilon^2) + b^2 (\varepsilon^3 + \varepsilon^4) = 0$$

cioè

$$\frac{a^2}{b^2} = -\frac{\varepsilon^3 + \varepsilon^4}{1 + \varepsilon^2} = \frac{(\varepsilon^4 - \varepsilon)^2}{(\varepsilon^2 - \varepsilon^3)^2} \qquad (**)$$

Possiamo dunque porre $a = \varepsilon^4 - \varepsilon$; $b = \pm (\varepsilon^2 - \varepsilon^3)$

e siccome cangiando z in $-z$ non si alterano $\mathcal{S}$, $\mathcal{U}$ mentre si cangia in $\mathcal{T}$ il segno di b, potremo assumere senz' altro per $\mathcal{T}$ la forma

$$\mathcal{T}) \quad z' = \frac{(\varepsilon^4 - \varepsilon) z + (\varepsilon^2 - \varepsilon^3)}{(\varepsilon^2 - \varepsilon^3) z - (\varepsilon^4 - \varepsilon)}$$

(*) Naturalmente non può essere $a = -d = 0$, $b = -c$ altrimenti $\mathcal{T}$ coinciderebbe con $\mathcal{U}$

(**) Basta ricordare l' identità $\varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0$

Combinando S, T, U e le loro potenze ne concludiamo che ai gruppi del V^2 tipo si può dare la forma normale:

gruppo dell' icosaedro e)

$$z' = \varepsilon^2 z, \quad -\frac{\varepsilon^2}{z}, \quad e^2\,\frac{(\varepsilon^4-\varepsilon^3)\varepsilon^3 z-(\varepsilon^4-\varepsilon)}{(\varepsilon^4-\varepsilon)\varepsilon^3 z+(\varepsilon^2-\varepsilon^3)}, \quad -\varepsilon^2\,\frac{(\varepsilon^2-\varepsilon^3)\varepsilon^3 z-(\varepsilon^4-\varepsilon)}{(\varepsilon^4-\varepsilon)\varepsilon^3 z+(\varepsilon^2-\varepsilon^3)}$$

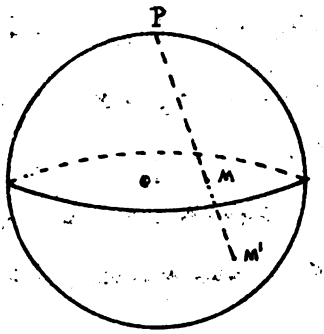
Ed è facile verificare che queste 60 sostituzioni lineari formano in effetto un gruppo.—

§ 49.— **La sfera complessa**.— Le ricerche dei § precedenti ci hanno dimostrato come ad ogni soluzione della equazione d' analisi indeterminata A) § 43 corrispondono gruppi di sostituzioni lineari effettivamente esistenti, ad ogni soluzione corrispondendo un unico tipo.— Ora questi gruppi possono ricevere una notevolissima rappresentazione geometrica che li collega ai **poliedri regolari** e che dà appunto ragione della loro denominazione di **gruppi dei poliedri regolari**.— Per occuparci di questa rappresentazione conviene prima che sostituiamo al piano di Gauss, come superficie sulla quale sono distesi i valori di una variabile complessa z, la **sfera complessa**, ciò che si fa nel modo seguente.—

Preso un sistema di assi cartesiani ortogonali $O\xi$, $O\eta$, $O\zeta$ distribuiamo sul piano $\xi\eta$, al modo di Gauss i valori della variabile complessa

$$z = x + i y .$$

Descriviamo col centro nell' origine la sfera di raggio $= 1$ che avrà per equazione $\xi^2 + \eta^2 + \zeta^2 = 1$



e riportiamo i valori di z da ogni punto $M \equiv (x, y)$ del piano $\xi\eta$ in quel punto $M' \equiv (\xi, \eta, \zeta)$ della sfera che si ottiene proiettando dal punto fisso (polo)

$$P \equiv (0, 0, 1)$$

della sfera il punto M sulla sfera stessa.. Per tal modo i punti interni al cerchio equatoriale verranno proiettati sull' emisfero inferiore, quelli esterni sull' emisfero superiore mentre i punti all' infinito del piano si raccoglieranno, in proiezione, nel polo P (*) e faremo così corrispondere biunivocamente le posizioni di un punto sulla sfera ai vari

---

(*) Questa proiezione della sfera sul piano dicesi la proiezione stereografica polare..

ri della variabile complessa z. La sfera rappresentativa si dirà, per abbreviare, la **sfera complessa**; i suoi due poli saranno il punto $z = \infty$ (polo di proiezione) col il polo opposto $z = 0$

Supponiamo ora che la sfera complessa si muova sopra se stessa, restando fisso il centro. Se indichiamo con z il valore della variabile complessa in un punto qualunque Q della sfera, con z' quello che si ha nel punto Q' ove Q si trasporta pel movimento, dobbiamo dimostrare il teorema fondamentale:

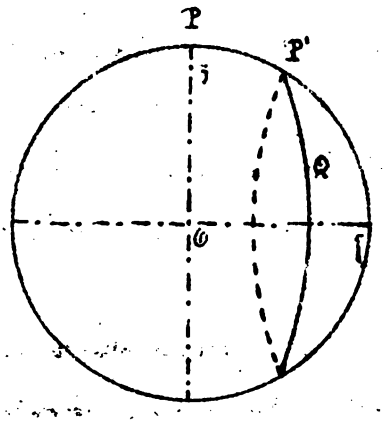
Ogni movimento della sfera in sè medesima è rappresentato da una sostituzione lineare

$$z' = \frac{az + b}{cz + d}$$

sulla variabile complessa. Diciamo subito che queste sostituzioni lineari hanno, come si vedrà, una forma speciale. Per dimostrare elementarmente il nostro teorema conviene premettere le osservazioni seguenti.

I movimenti di una sfera in sè stessa sono operazioni suscettibili di composizione e noi vogliamo in primo luogo dimostrare che ogni tale movimento può

composti con tre successive rotazioni attorno agli assi coordinati $O\xi$, $O\eta$, $O\zeta$. E infatti ogni punto Q della sfera con due rotazioni attorno ad $O\xi$, $O\eta$ rispettivamente può trasportarsi nel polo P. E invero se



conduciamo per Q il piano normale all'asse $O\xi$ e chiamiamo P' uno dei due punti ove il circolo minore sezione colla sfera di detto piano incontra il meridiano del piano $O\xi\zeta$, con una rotazione attorno ad $O\xi$ si porterà Q in P' e con una attorno ad $O\eta$ si porterà P' in P. Ciò posto sia S un movimento della sfera che porta il polo P in un punto Q; con due successive rotazioni

$$U_\xi, \quad U_\eta$$

attorno ad $O\xi$, $O\eta$ possiamo riportare Q in P. Il movimento composto

$$S\, U_\xi\, U_\eta$$

lascia fisso P (quindi il polo opposto) ed è dunque una rotazione U_ζ attorno all'asse $O\zeta$ e si ha perciò

$S' = U_3 U_\eta^{-1} U_\xi^{-1}$.–

§50.– Formola di Cayley.–

Per dimostrare il teorema enunciato nel § precedente basterà provare che ogni rotazione nella sfera complessa attorno ad uno degli assi coordinati è rappresentata da una sostituzione lineare sulla variabile complessa z giacchè il risultato di più sostituzioni lineari successive è nuovamente una sostituzione lineare.– Scriviamo in primo luogo le formole di corrispondenza fra un punto $M \equiv (x,y)$ del piano equatoriale e il suo punto proiezione $M' \equiv (\xi, \eta, \zeta)$ sulla sfera; esse sono (*)

$$(1)\quad x = \frac{\xi}{1-\zeta}\ ,\quad y = \frac{\eta}{1-\zeta}\ ,\quad z = x + iy = \frac{\xi + i\eta}{1-\zeta}$$

$$(2)\quad \xi = \frac{2x}{1+x^2+y^2}\ ,\quad \eta = \frac{2y}{1+x^2+y^2}\ ,\quad \zeta = \frac{x^2+y^2-1}{1+x^2+y^2}\ .–$$

È utile scrivere queste ultime sotto un'altra forma introducendo la variabile complessa coniugata di z che è

(*) Per verità si osservi che indicando con $\frac{m}{n}$ il rapporto secondo cui il punto $M \equiv (x, y, 0)$ divide il segmento compreso fra $P \equiv (0, 0, 1)$ e $M' \equiv (\xi, \eta, \zeta)$ deve aversi

$$m\xi + n = 0\ ,\ \text{onde}\quad m : n = 1 : -\zeta\ .–$$

Indicando la variabile complessa coniugata di z che indicheremo con z_0:

$$z_0 = \frac{\xi - i\eta}{1 - \zeta} ;$$

allora le (2) si scrivono

$$(2^*) \qquad \xi = \frac{z + z_0}{zz_0 + 1} , \quad \eta = \frac{1}{i}\frac{z - z_0}{zz_0 + 1} \qquad \zeta = \frac{zz_0 - 1}{zz_0 + 1}$$

Ciò posto, consideriamo:

1° una rotazione nel senso positivo di ampiezza α attorno all'asse $O\zeta$. Indicando con (ξ', η', ζ') il punto in cui si trasporta (ξ, η, ζ) dopo il movimento, avremo

$$\xi' = \xi \cos\alpha - \eta \operatorname{sen}\alpha$$

$$\eta' = \xi \operatorname{sen}\alpha + \eta \cos\alpha$$

$$\zeta' = \zeta$$

onde $$z' = \frac{\xi' + i\eta'}{1 - \zeta'} = \frac{(\cos\alpha + i \operatorname{sen}\alpha)(\xi + i\eta)}{1 - \zeta} = e^{i\alpha} z$$

formola che si conviene scrivere, dando al determinante della sostituzione il valore 1:

$$(\alpha) \qquad z' = \frac{\left(\cos\frac{\alpha}{2} + i \operatorname{sen}\frac{\alpha}{2}\right) z}{\cos\frac{\alpha}{2} - i \operatorname{sen}\frac{\alpha}{2}} .$$

2°) una rotazione d'ampiezza α, in senso positivo, attorno all'asse $O\xi$.

Avremo $\xi' = \xi$ $\qquad \eta' = \eta\cos\alpha - \zeta\operatorname{sen}\alpha$

$$\zeta' = \eta \operatorname{sen}\alpha + \zeta \cos\alpha$$

inoltre

$$z' = \frac{\xi' + i\eta'}{1 - \zeta'} = \frac{\xi + i(\eta\cos\alpha - \zeta\sin\alpha)}{1 - \eta\sin\alpha - \zeta\cos\alpha}$$

e sostituendo per ξ, η, ζ i loro valori (2*)

$$z' = \frac{z + z_0 + \cos\alpha(z - z_0) - i\sin\alpha(zz_0 - 1)}{zz_0 + 1 + i\sin\alpha(z - z_0) - \cos\alpha(zz_0 - 1)} ;$$

sopprimendo dal numeratore e denominatore in questa ultima formola il fattore comune

$$2\left(\cos\frac{\alpha}{2} - i\sin\frac{\alpha}{2}z_0\right)$$

troviamo

$$(3) \qquad z' = \frac{\cos\frac{\alpha}{2}z + i\sin\frac{\alpha}{2}}{i\sin\frac{\alpha}{2}z + \cos\frac{\alpha}{2}} \ldots$$

3° consideriamo in fine: una rotazione d'ampiezza α attorno all'asse $O\eta$; avremo

$$\begin{cases} \eta' = \eta \\ \zeta' = \zeta\cos\alpha - \xi\sin\alpha \\ \xi' = \zeta\sin\alpha + \xi\cos\alpha \end{cases}$$

e sarà

$$z' = \frac{\zeta\sin\alpha + \xi\cos\alpha + i\eta}{1 - \zeta\cos\alpha + \xi\sin\alpha} ,$$

onde sostituendo i valori (2*) e supponendo il fattore

$$2\left(\sin\frac{\alpha}{2}z_0 + \cos\frac{\alpha}{2}\right)$$

comune al denominatore e numeratore otteniamo

$$(\gamma) \qquad z' = \frac{\cos\frac{\alpha}{2}z - \operatorname{sen}\frac{\alpha}{2}}{\operatorname{sen}\frac{\alpha}{2}z + \cos\frac{\alpha}{2}}$$

Così è dimostrato che qualunque movimento della sfera complessa in sé medesima è rappresentato analiticamente da una sostituzione lineare sulla variabile complessa z. — Di più possiamo ora facilmente vedere quale forma avranno i coefficienti A, B, C, D di una tale sostituzione

$$z' = \frac{Az + B}{Cz + D}$$

Infatti le tre sostituzioni elementari $(\alpha), (\beta), (\gamma)$ mediante le quali ogni tale sostituzione può comporsi hanno il determinante eguale all'unità mentre D è coniugato di A e C di $-B$, talchè indicando con A_0 la quantità complessa coniugata di A con B_0 la coniugata di B, una qualunque delle $(\alpha)(\beta)(\gamma)$ ha la forma

$$(I) \qquad z' = \frac{Az + B}{-B_0 z + A_0}, \qquad AA_0 + BB_0 = 1$$

Ora si vede subito che due qualunque sostituzioni della forma (I), composte fra loro, danno nuovamente una sostituzione della forma stessa e se ne conclude quindi: Qualunque movimento della sfera complessa in sé medesima è rappresentato da una sostitu-

zione lineare della forma (I) (formola di Cayle) si potrebbe dimostrare inversamente che una qualunque sostituzione (I) rappresenta un movimento della sfera complessa in sè stessa.(*)

Qui osserviamo ancora che in ogni movimento (I) della sfera vi sono due punti che rimangono fissi e cioè i due punti della sfera corrispondenti ai valori di z radici della equazione di 2° grado

$$B_0 z^2 + (A - A_0) z + B = 0$$

Ora se z è una delle radici, l'altra è $-\frac{1}{z_0}$ come si vede subito, cangiando nella precedente i in $-i$ e le formole (2*) ci dimostrano subito che i due punti fissi si sono diametralmente opposti, come del resto è chiaro geometricamente. Se ne deduce il noto teorema: Ogni movimento della sfera in sè stessa è una rotazione attorno ad un diametro.

§ 51. **Movimenti di 2ª specie.** Insieme a quelle trasformazioni della sfera in sè stessa che cor-

---

(*) Basta perciò far vedere che una sostituzione (I) può comporsi con tre successive sostituzioni $(\alpha)(\beta)(\gamma)$.

servano l'eguaglianza diretta delle figure sferiche già va talora considerare anche quelle trasformazioni per le quali le figure corrispondenti sono inversamente eguali; una tale trasformazione si dirà un movimento improprio o di 2ª specie. Quale sarà la rappresentazione analitica di un movimento di 2ª specie? La formola

$$z' = z_0$$

rappresenta per le (2*) un movimento di 2ª specie e precisamente una simmetria rispetto al piano ξz e combinandosi con questo il più generale movimento di 1ª specie dato dalla formola (I) del Cayley, avremo la formola

$$(1^*) \qquad z' = \frac{A z_0 + B}{-B_0 z_0 + A_0}, \quad A A_0 + B B_0 = 1$$

che ci rappresenterà il più generale movimento di 2ª specie.

Tra questi movimenti meritano particolare interesse quelli a periodo 2; per trovarli osserviamo che l'inversa della (I*) è data da

$$z' = \frac{A z_0 - B_0}{B z_0 + A_0}$$

e coincide colla (I*) solo quando si abbia

$$B = -B_0$$

cioè quando sia B puramente immaginario, ovvero quando

sia $\qquad A = 0 \qquad B = B_0 = \pm 1$

Nel 1° caso se ricerchiamo quali punti della sfera restano fissi, vediamo che essi debbono soddisfare la condizione

$$B z z_0 + A_0 z - A z_0 + B_0 = 0$$

cioè ponendo $\quad A = a_1 + i a_2 \quad , \quad B = i b \quad$ con a_1, a_2, b reali e $\quad a_1^2 + a_2^2 + b^2 = 1$, all'altra

$$b(z z_0 - 1) - a_2(z + z_0) + \frac{a_1}{i}(z - z_0) = 0$$

che osservando le (2^*) ci dà

$$(3) \qquad -a_2 \xi + a_1 \eta + b \zeta = 0$$

equazione di un piano che passa pel centro.– Dunque per questo movimento di 2ª specie rimangono fissi tutti i punti della sfera situati sul circolo massimo intersezione del piano (3) colla sfera; il movimento non è che una **riflessione** su questo circolo massimo.– Nel secondo caso invece si ha il movimento di 2ª specie

$$z' = -\frac{1}{z_0} \, ,$$

che diremo **inversione**, semplicemente (per le (2^*)) consiste nel sostituire ad ogni punto della sfera il punto diametralmente opposto.– È questo l'unico movimento di 2ª specie a periodo 2, pel quale nessun punto della sfera rimane fisso.–

È bene poi osservare che: **Per qualsiasi movimen-**

to di 2ª specie, che non sia una riflessione, tutti i punti della sfera cangiano di posto. E invero se rimanesse fisso un punto tale rimarrebbe il diametralmente opposto e vi sarebbe un movimento simile che lascierebbe fissi i poli $z=0$, $z=\infty$; un tale movimento è rappresentato dalla sostituzione a periodo 2:

$$z' = \frac{A}{A_0} z,$$

che è una riflessione.

§ 52. — **Gruppi di rotazioni.** — Dalle ricerche precedenti risulta che se un certo numero di rotazioni della sfera complessa in sè stessa formano un gruppo, formeranno pure un gruppo (isomorfo) le sostituzioni lineari che a queste corrispondono secondo la formula di Cayley (I); un tale gruppo, ove consti di un numero finito di operazioni, dovrà necessariamente rientrare in uno dei cinque tipi precedentemente studiati. Dimostreremo ora la esistenza di gruppi di rotazioni di ciascuno dei cinque tipi e stabiliremo così la rappresentazione geometrica cercata.(*)

(*) Si potrebbe anche dare una dimostrazione diretta di

Consideriamo un poliedro regolare inscritto o circoscritto alla sfera complessa.- Con una rotazione della sfera possiamo sovrapporre il poliedro a sé stesso e precisamente possiamo portare uno spigolo fisso del poliedro sopra un altro spigolo qualunque in due modi diversi.- Il numero N di queste rotazioni distinte (l'identità compresa) è quindi eguale al doppio del numero degli spigoli del poliedro ed è evidente che queste rotazioni formano un gruppo perchè sono tutte e sole quelle rotazioni che riportano il poliedro in se stesso (*)

Dei cinque poliedri regolari basta considerarne tre poichè due poliedri polari l'uno dell'altro (ottaedro e cubo), (icosaedro e dodecaedro) danno luogo al medesimo gruppo come si vede subito osservando che i piani tangenti nei vertici di un poliedro

---

questo fatto, osservando che ciascuna sostituzione generatrice di un gruppo del tipo normale (§ 45 - 48) si può porre sotto la forma (I) di Cayley.-

(*) L'ordine N di questo gruppo si può anche valutare così: se il poliedro ha f facce n-latere e v vertici con angoli solidi a r facce sarà $N = 2S = fn = vr$.-

possono assumersi come faccie del poliedro polare. Avremo dunque tre gruppi di rotazioni corrispondenti rispettivamente al tetraedro, ottaedro ed icosaedro e corrispondenti rispettivamente 12, 24 e 60 rotazioni; questi sono evidentemente i gruppi del tipo III), IV), V).

Ma possiamo facilmente trovare anche i gruppi di rotazioni corrispondenti al tipo I) e II). Basta perciò considerare i solidi seguenti:

1° Una piramide regolare con un numero qualunque n di faccie laterali, la cui base sia inscritta nel circolo equatoriale e il cui vertice sia il polo P della sfera

2° Una doppia piramide regolare ottenuta rimenando alla precedente piramide la simmetrica rispetto al piano equatoriale.

Il primo solido si sovrappone a sè stesso per un gruppo (ciclico) di rotazioni generato dalla rotazione S d'ampiezza $= \frac{2\pi}{n}$ attorno all'asse polare. Il secondo, oltre che dalle precedenti rotazioni, è ricondotto in sè stesso dalle n rotazioni d'ampiezza $= \pi$ (ribaltamenti) che dal centro vanno ai vertici e ai punti medii dei lati della base comune alle due piramidi.

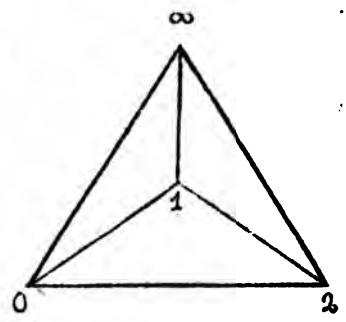
I gruppi corrispondenti di sostituzioni appartengono precisamente ai tipi I) e II).–

§ 53.– Gruppi di rotazioni del tetraedro e dell' ottaedro.–

Esaminiamo ora come nei gruppi di rotazioni dei tre poliedri regolari si realizzano geometricamente le circostanze che abbiamo già discusse analiticamente nell' enumerazione dei diversi tipi (§ 44).– Il gruppo tetraedrale consta di $2 \times 6 = 12$ rotazioni fra le quali figurano 3 rotazioni a periodo 2 attorno alle tre congiungenti i punti medi delle coppie opposte; queste tre congiungenti incontrano la sfera in 6 punti che figurano al punto come i 6 poli di 2° ordine corrispondenti a $\nu_1 = 2$.– Abbiamo poi 8 rotazioni a periodo 3 attorno alle quattro congiungenti i vertici coi punti medii delle facce opposte e i poli di queste rotazioni si dividono in due classi di poli equivalenti, cioè i 4 vertici ed i 4 punti diametralmente opposti corrispondentemente ai valori $\nu_2 = 3$ $\nu_3 = 3$ di ν_2, ν_3.– L' isomorfismo oloedrico del gruppo tetraedrale col gruppo alterno su quattro elementi è già reso evidente dal

Fatto che i quattro vertici (o le quattro facce) vengono permutati fra loro in 12 modi diversi. — Si può anche rappresentare analiticamente il gruppo sui quattro vertici distinti cogli indici $0, 1, 2, \infty$ come il gruppo modulare per $p = 3$ $(\S 40)$

$$\nu' \equiv \frac{\alpha\nu + \beta}{\gamma\nu + \delta}, \quad \alpha\delta - \beta\gamma \equiv 1 \pmod 3$$



Scrivendo per esteso le 12 sostituzioni si abbiamo

rotazioni a periodo 3 : $\nu' = \nu + 1$, $(0\,1\,2)$,

(sostituzioni paraboliche) : $= \nu + 2$, $\frac{\nu}{\nu+1}$, $\frac{\nu}{2\nu+1}$, $\frac{2}{\nu+1}$, $\frac{\nu+1}{2\nu}$

$(0\,2\,1)$, $(\infty\,1\,2)$, $(\infty\,2\,1)$, $(0\,2\,\infty)$, $(0\,\infty\,2)$

$= \frac{\nu+2}{\nu}$, $\frac{1}{2\nu+1}$. —

$(0\,\infty\,1)$, $(0\,1\,\infty)$

rotazioni a periodo 2: $\nu' = -\frac{1}{\nu}$, $\frac{1-\nu}{1+\nu}$, $\frac{1+\nu}{-1+\nu}$. —

(sostituzioni iperboliche) $(\infty\,0)(1\,2)$, $(0\,1)(2\,\infty)$, $(0\,2)(1\,\infty)$

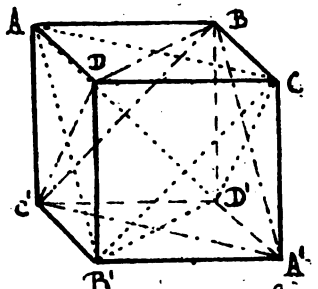
Queste ultime tre, che sono ribaltamenti attorno a tre assi ortogonali, insieme all'identità formano il sottogruppo G_4 (Vierergruppe) invariante in G_{12}. —

Passiamo al gruppo dell'ottaedro o cubo. — Riferendoci p.es. al cubo, avremo 9 rotazioni di periodo 4 attorno alle tre congiungenti i centri delle facce opposte,

8 rotazioni a periodo 3 attorno alle quattro diagonali, 6 rotazioni di periodo 2 attorno alle sei congiungenti i punti medii delle costole parallele opposte ed in fine l'identità ($3+3+6+1=24$). — Le quattro diagonali del cubo vengono permutate fra loro in 24 modi diversi, il che dà l'immagine geometrica dell'isomorfismo del gruppo ottaedrale col gruppo totale su quattro elementi ovvero col gruppo lineare totale

$$\nu' \equiv \frac{\alpha\nu+\beta}{\gamma\nu+\delta} \pmod 3 .$$

Osserviamo poi che gli otto vertici del cubo si distribuiscono in due sistemi di quattro come vertici di due tetraedri regolari $ACB'D'$, $A'C'BD$ e le 24 rotazioni del gruppo o lasciano fermo ciascun tetraedro o scambiano l'un tetraedro coll'altro. — Le prime, in numero di 12, formano nel gruppo ottaedrale il sottogruppo invariante tetraedrale. —



§ 54. — **Gruppo dell'icosaedro.** — L'icosaedro ha 12 vertici, 20 faccie e 30 spigoli. — Il suo gruppo consta di 60 rotazioni che si ripartiscono così: 1° 24 rotazioni a

periodo 5 attorno alle sei congiungenti i vertici opposti (diametri).

2°) rotazioni a periodo 3 attorno alle dieci congiungenti i centri delle faccie parallele opposte

3°) 15 rotazioni a periodo 2 attorno alle quindici congiungenti i punti medii delle costole parallele opposte

4°) l' identità ($24 + 20 + 15 + 1 = 60$)

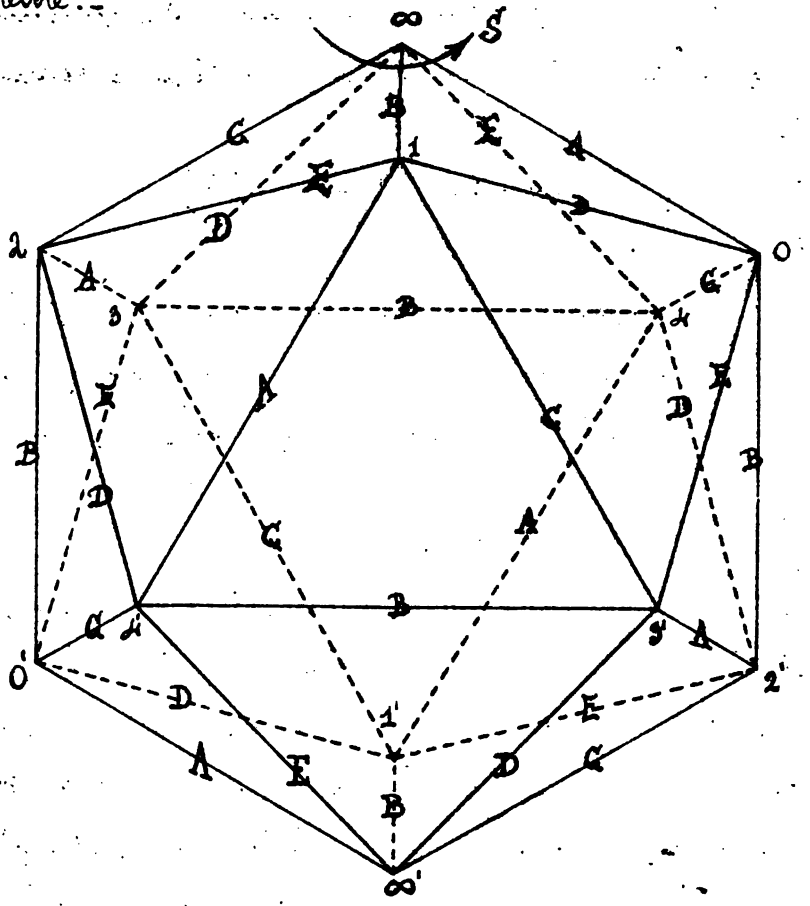
I sei diametri dell' icosaedro vengono permutati fra loro secondo 60 sostituzioni di un gruppo transitivo semplice, che coincide adunque col gruppo modulare $p = 5$. — Ciò si conferma geometricamente così: Distinguiamo i sei diametri cogli indici

$$\infty, 0\ 1, 2, 3, 4$$

come è indicato sulla figura qui retro pei vertici corrispondenti e consideriamo la rotazione S di ampiezza $= \frac{2\pi}{5}$ attorno al diametro $\infty\,\infty'$ nel senso della freccia e la rotazione T di ampiezza $= \pi$ attorno alla congiungente i punti medii degli spigoli opposti $\overline{\infty 0}$, $\overline{\infty' 0'}$. — Sopra i sei diametri la rotazione S produce la sostituzione

$$(0\ 1\ 2\ 3\ 4) \quad \text{ossia} \quad \nu' \equiv \nu + 1 \pmod 5$$

e la I l'altra $(0\,\infty)(1\,4)$ ossia $\nu' \equiv -\frac{1}{\nu} \pmod 5$
queste sono le sostituzioni generatrici del gruppo modulare $(5,1,0)$ e però colle rotazioni S, T si genera tutto il gruppo icosaedrale, come è facile vedere anche geometricamente.



Si può osservare l'isomorfismo del gruppo icosaedrale col gruppo alterno su 5 elementi direttamente sulla fi-

guna nel modo seguente. I 30 spigoli dell'icosaedro possono ripartirsi in 5 sistemi di 6 spigoli ciascuno, in guisa che ogni sistema consti di due terne ortogonali, gli spigoli di una terna essendo paralleli a quelli dell'altra. — Per ottenere questa distribuzione degli spigoli in sistemi basta osservare la piramide regolare a base pentagonale che si forma ad ogni angolo solido dell'icosaedro; ad ogni lato (spigolo) del pentagono base appartiene, nel medesimo sistema, lo spigolo laterale opposto. — Distinguendo i cinque sistemi colle lettere A, B, C, D, E, attribuiamo nella figura qui sotto ad ogni spigolo la lettera del sistema cui appartiene. —

Vediamo allora che le rotazioni elementari S, T del gruppo icosaedrale producono sui cinque sistemi A, B, C, D, E le sostituzioni elementari del gruppo alterno

$$S \sim (A\,B\,C\,D\,E)$$

$$T \sim (B\,C)(D\,E)$$

e però le 60 rotazioni del gruppo icosaedrale producono sui cinque sistemi A, B, C, D, E le 60 sostituzioni del gruppo alterno.

Invece dei cinque sistemi di spigoli possiamo considerare come elementi cinque ottaedri regolari poiché i sei punti medii degli spigoli di un medesimo sistema sono appunto

i vertici di un ottaedro regolare. — Le rotazioni del gruppo icosaedrale che lasciano fisso uno degli ottaedri formano un gruppo tetraedrale entro il quale abbiamo un Dierergrup= po i cui tre assi sono le diagonali dell' ottaedro. — Il grup= po icosaedrale contiene quindi 5 di questi sottogruppi del 4° ordine che sono fra loro affini (teorema di Sylow).

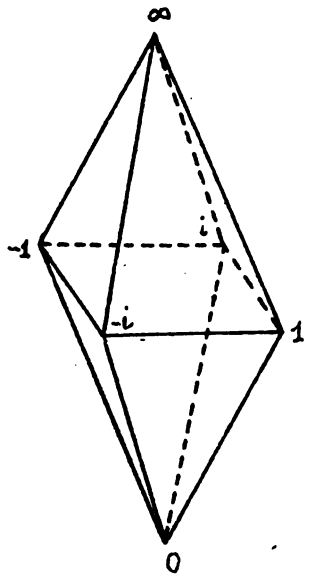
§ 55. — Orientazione dei poliedri regolari corrispondente alla forma normale dei grup= pi. — Dalle nostre ricerche risulta che è possibile dare ai solidi regolari tale orientazione entro la sfera complessa che le rotazioni del loro gruppo, tradotte in sostituzioni lineari secondo la formola di Cayley, diano luogo alle for= me normali dei gruppi (§ 45 - 48). —

Pei gruppi ciclici si ottiene tale coincidenza inscrivendo la base della piramide regolare nel cerchio equatoriale e fa= cendo quindi il vertice nel punto $z = \infty$ ovvero in $Z = 0$.

Pei gruppi del secondo tipo basta situare i due vertici della doppia piramide in $Z = 0$ e $Z = \infty$ ed inoltre un vertice della base in $Z = i$. —

Il gruppo del tetraedro essendo contenuto come sottogrup= po (invariante) nel gruppo dell' ottaedro basterà occupar=

ci di quest' ultimo. Otteniamo la forma normale d) §17 per questo gruppo semplicemente col far coincidere le tre diagonali dell' ottaedro coi tre assi coordinati, onde due dei vertici si trovano in $z = 0$, $z = \infty$



e gli altri quattro sul cerchio equatoriale in

$$z = \pm 1 \quad , \quad z = \pm i$$

Allora le sostituzioni

$$z' = i^{\varepsilon} z$$

rappresentano le rotazioni attorno al diametro $0\ \infty$, le sostituzioni $z' = \frac{i^{\varepsilon}}{z}$ danno i ribaltamenti attorno agli assi 0ξ, 0η ed alle loro bisettrici e l' altra

$$z' = i\,\frac{z+1}{z-1}$$

rappresenta la rotazione di $\frac{2\pi}{3}$ attorno alla congiungente i centri delle due faccie

$$(0, -i, -1) \qquad (\infty, i, 1)$$

Componendo fra loro si hanno le 24 sostituzioni d) del gruppo ottaedrale.

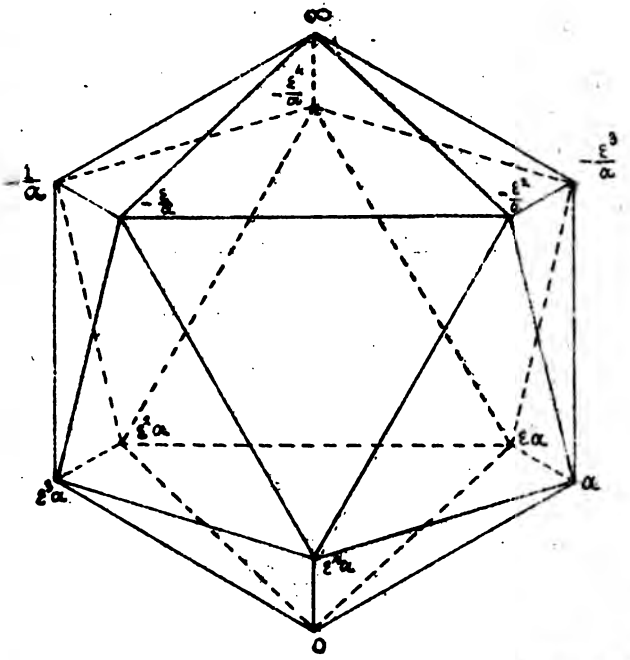
Per l' icosaedro sistemiamolo in primo luogo in guisa che

due vertici opposti siano in

$$z = 0 \quad , \quad z = \infty$$

e la rotazione S di $\frac{2\pi}{5}$ attorno al diametro che li congiunge sarà data da

$$z' = \varepsilon z \quad , \qquad \varepsilon = e^{\frac{2\pi i}{5}}$$



Supponiamo in secondo luogo che uno dei cinque vertici equidistanti dal vertice $z=0$ si collochi sul piano $\{\zeta\}$ dalla parte delle ζ positive. Se indichiamo con $z = a$ il valore della variabile complessa in questo vertice, sarà a reale positiva e minore dell'unità; i cinque vertici circostanti a $z=0$ saranno

$$z = a \; , \; \varepsilon a \; , \; \varepsilon^2 a \; , \; \varepsilon^3 a \; , \; \varepsilon^4 a \; .$$

e nei cinque opposti avremo

$$x = -\frac{1}{a}\ ,\ -\frac{\varepsilon}{a}\ ,\ -\frac{\varepsilon^2}{a}\ ,\ -\frac{\varepsilon^3}{a}\ ,\ -\frac{\varepsilon^4}{a}$$

Se consideriamo la rotazione T a periodo 2 attorno alla congiungente i punti medii dei due spigoli opposti $(\overline{0,a})$ $(\overline{\infty, -\frac{1}{a}})$, essa avrà per espressione analitica

$$x' = \frac{a - x}{ax + 1}$$

e poichè d'altronde essa deve scambiare εa con $\varepsilon^4 a$ sarà

$$\varepsilon^4 = \frac{1 - \varepsilon}{\varepsilon a^2 + 1}$$

onde

$$a^2 = 1 - \varepsilon - \varepsilon^4 = (\varepsilon + \varepsilon^4)^2$$

e però

$$a = \varepsilon + \varepsilon^4$$

Ne segue per T l'espressione

$$T) \qquad x' = \frac{\varepsilon + \varepsilon^4 - x}{(\varepsilon + \varepsilon^4) + 1} = \frac{(\varepsilon^4 - \varepsilon)x + \varepsilon^2 - \varepsilon^3}{(\varepsilon^2 - \varepsilon^3)x - (\varepsilon^4 - \varepsilon)}\ .$$

Le espressioni S, T sopra costruite sono appunto quelle delle sostituzioni generatrici del gruppo icosaedrale sotto la forma normale del § 48.-

§56.- **Gruppi ampliati**.- Trattiamo ora rapidamente il problema di determinare i gruppi finiti di movimenti di prima e seconda specie della sfera in se stessa.- Un tale gruppo $\mathfrak{G}$ contiene necessariamente

tanti movimenti di prima quanti di seconda specie e quelli di prima formano un sottogruppo T d'indice 2 invariante in G. Questo sottogruppo T appartiene come è chiaro ad uno dei cinque tipi di gruppi poliedrali che abbiamo sopra studiato. Per trovare dunque tutti questi gruppi G basta esaminare ciascun gruppo poliedrale T e ampliarlo con un movimento t di 2ª specie che trasformi T in sè stesso mentre t^2 appartiene a T; allora sarà $G = (T, tT)$ uno dei gruppi richiesti.

È facile costruire tutti questi gruppi discutendo i cinque casi corrispondenti per T. Noi qui ci limitiamo al caso in cui T appartiene al 4° o 5° tipo, cioè è il gruppo dell'ottaedro o dell'icosaedro.

Un movimento t di 2ª specie che trasformi il gruppo ottaedrale od icosaedrale in sè stesso deve trasformare le rotazioni del gruppo in rotazioni della medesima specie appartenenti al gruppo e poichè i poli di queste rotazioni sono unicamente i vertici del poliedro, dovrà trasformare il poliedro in sè stesso (*).

(*) Nel caso del tetraedro invece bisogna avere riguardo anche

ora associando t con una rotazione S del gruppo si può sempre far sì che il movimento

$$t' = tS$$

porti un vertice nell'opposto e quindi tutti gli altri vertici negli opposti, onde t' non è che l'inversione cui ha la forma

$$z' = -\frac{1}{z_0}$$

così otteniamo tanto nel caso dell'ottaedro quanto in quello dell'icosaedro un solo gruppo ampliato. — Quante riflessioni contiene questo gruppo? Siccome l'inversione t è permutabile con qualunque movimento, sarà a periodo 2 il movimento di 2ª specie tS quando lo sia S e viceversa, se S è un ribaltamento, la tS sarà una riflessione sul cerchio massimo il cui piano è normale all'asse di ribaltamento. Così dunque avremo nel gruppo ampliato dell'ottaedro **nove** riflessioni — in quello dell'icosaedro **quindici**; i piani di queste riflessioni sono i piani di simmetria dell'ottaedro e

---

all'altra possibilità che il tetraedro venga trasformato in quello opposto (che ha i vertici opposti a quelli del primo), onde due possibili ampliamenti. —

dell' icosaedro. I corrispondenti circoli di riflessione dividono la sfera rispettivamente in 48 e 120 triangoli sferici alternatamente congruenti e simmetrici con angoli di $\frac{\pi}{3}, \frac{\pi}{4}, \frac{\pi}{2}$ nel primo caso e nel secondo con angoli di $\frac{\pi}{3}, \frac{\pi}{5}, \frac{\pi}{2}$. Si ottiene uno di questi triangoli congiungendo con archi di circolo massimo i tre vertici di una faccia del poliedro regolare e suddividendo poi questo triangolo equilatero in sei triangoli minori per mezzo delle tre altezze sferiche. Queste reti di triangoli congruenti in cui risulta divisa la sfera diconsi la rete ottaedrica e la rete icosaedrica. I movimenti del gruppo ampliato sono quelli che riportano la rete in se medesima.

Indice
della prima parte

§1. — Sostituzioni e loro composizione. pag. 3.
2. — Periodo di una sostituzione. " 6
3. — Sostituzioni circolari. " 9.
4. — Trasposizioni. " 11.
5. — Sostituzioni simili — permutabili. " 15.
6. — Gruppi di sostituzioni " 17.
7. — Teorema fondamentale " 19.
8 — Gruppo alterno " 23.
9. — Gruppi transitivi ed intransitivi " 25.
10. — Teoremi sui gruppi transitivi " 29.
11. — Limite del grado di transitività " 32.
12. — Gruppi imprimitivi e primitivi " 35.
13. — Teorema " 37.
14. — Gruppi isomorfi " 40.
15. — I gruppi generali di operazioni " 43.
16. — Sottogruppi invarianti " 45.
17. — Gruppi semplici e composti " 49.

§ 18. – Serie di composizione – Teorema di Jordan pag. 53.
19. – Serie di composizione di gruppi isomorfi » 56.
20. – Sottogruppi invarianti del gruppo totale » 58.
21. – Semplicità del gruppo alterno per $n \neq 4$ » 60.
22. – Serie di composizione principale » 64.
23. – Gruppi fattoriali e teorema di Holder » 68.
24. – Gruppi complementari » 70.
25. – Il primo teorema di Sylow » 73.
26. – Il secondo teorema di Sylow » 78.
27. – Dimostrazione » 82.
28. – Gruppi di ordine p^α » 85.
29. – Gruppi semplici degli ordini da 1 a 100 » 87.
30. – Gruppi semplici d'ordine uguale a 60 » 91.
31. – Gruppi Abeliani » 92.
32. – Base di un gruppo Abeliano » 96.
33. – Invarianti di un gruppo Abeliano » 99.
34. – Gruppi transitivi risolubili sopra un numero primo di elementi » 103.
35. – Gruppo metaciclico » 106.
36. – Rappresentazione analitica delle sostituzioni del gruppo metaciclico » 109.
37. – Serie di composizione del gruppo metaciclico » 111.

§ 38.- Gruppo lineare totale sopra $p+1$ indici pag. 113.
39.- Periodo delle sostituzioni del gruppo lineare totale " 118.
40.- Sostituzioni generatrici del gruppo modulare " 121.
41.- Il gruppo modulare per $p>3$ è semplice " 125.
42.- Gruppi di sostituzioni lineari sopra una var.ta " 129.
43.- Poli delle sostituzioni di un gruppo finito " 132.
44.- Enumerazione dei possibili tipi " 136.
45.- Gruppi ciclici e diedrali " 138.
46.- Gruppo del tetraedro " 142.
47.- Gruppo dell' ottaedro " 145.
48.- Gruppo dell' icosaedro " 147.
49.- La sfera complessa " 152.
50.- Formola di Cayley " 156.
51.- Movimenti di 2ª specie " 160.
52.- Gruppi di rotazioni " 163.
53.- Gruppi di rotazioni del tetraedro e dell' ottaedro " 166.
54.- Gruppo dell' icosaedro " 168.
55.- Orientazione dei poliedri regolari corrispondente alla forma normale dei gruppi " 172.
56.- Gruppi ampliati " 175.

Parte seconda

Parte seconda

Teoria delle equazioni algebriche secondo Galois

§ 57. Irriducibilità. Prima di studiare le applicazioni della teoria dei gruppi alle questioni che concernono la risoluzione delle equazioni algebriche, conviene ritornare sopra alcuni concetti fondamentali dell'algebra per bene precisarne il senso.

Una funzione razionale intera

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$

di una variabile x dicesi **irriducibile** quando è impossibile scindere $f(x)$ nel prodotto di fattori di grado minore i cui coefficienti siano **razionalmente noti**.

Questo concetto d'irriducibilità non ha senso proprio se non quando venga fissato quali sono le quantità che si riguardano come razionalmente note, se non quando si fissi, come diremo con Kronecker, il campo di raziona-

lità. – Per definire il campo di razionalità basterà dare quelle quantità fondamentali

$$R, R', R'' \ldots\ldots\ldots$$

del campo stesso, per le quali tutte le altre, che si considerano come note, sono nel senso ordinario razionalmente esprimibili; allora il campo di razionalità, che indicheremo colla notazione di Kronecker

$$(R, R', R'' \ldots\ldots),$$

conterrà tutte e sole quelle quantità che sono funzioni razionali a coefficienti interi di $R, R', R'' \ldots\ldots$

Così formano un campo di razionalità gli ordinari numeri razionali e questo campo è evidentemente contenuto in qualsiasi altro campo di razionalità; esso si dirà perciò il campo **assoluto** di razionalità e si denoterà col simbolo $[1]$. – Così pure formano un campo di razionalità tutti i numeri della forma

$$a + b\sqrt{5}$$

essendo a, b frazioni ordinarie; qui si ha una sola quantità fondamentale nel campo e sarà $R = \sqrt{5}$. –

Quando parliamo della irriducibilità o meno di una funzione razionale intera $f(x)$, intendiamo naturalmente che i coefficienti della f debbono essere dati, cioè appartenenti al

campo di razionalità e in generale, se non si avverte esplicitamente il contrario, s'intenderà che il campo di razionalità del quale si parla sia quello determinato dai coefficienti di $f(x)$. Altrimenti bisognerà parlare della irriducibilità o riducibilità della f in un determinato campo $(R, R', R'' \ldots\ldots)$. — Se in particolare riuscirà conveniente considerare come note quantità le quali prima non si consideravano come tali, si dirà che tali quantità si aggiungono al campo di razionalità e le quantità stesse si diranno allora aggiunte. Ad ogni aggiunta di nuove quantità il campo di razionalità si amplia e naturalmente può darsi che una funzione $f(x)$ irriducibile nel campo primitivo diventi riducibile nel campo ampliato. Così $f(x) = x^2 - 7$ che è irriducibile nel campo assoluto di razionalità, diventa riducibile nel campo $(\sqrt{7})$. —

Precisato così il concetto d'irriducibilità delle funzioni razionali intere di una variabile (*), diremo che l'equazione

$$f(x) = a_0 x^n + a_1 x^{n-1} \ldots\ldots + a_{n-1} x + a_n = 0$$

è irriducibile in un determinato campo di razionalità $(R, R', R'' \ldots\ldots)$ se tale è la funzione $f(x)$. — Ed ora

---

(*) Le stesse considerazioni valgono per funzioni di più variabili. —

ricordiamo alcuni teoremi, ai quali dovremo continuamente ricorrere in seguito:

1° Se un'equazione $F(x)=0$ ammette una radice della equazione irriducibile $f(x)=0$, le ammette tutte. E infatti si determini il massimo comun divisore $\psi(x)$ di $F(x)$, $f(x)$, ciò che si fa con operazioni razionali, sicchè i coefficienti di $\psi(x)$ apparterranno all'attuale campo di razionalità. Se $\psi(x)$ non coincidesse (salvo un fattore costante) con $f(x)$ questa, ammettendo il divisore razionale $\psi(x)$, sarebbe riducibile e cioè:

2° Un'equazione irriducibile non può avere radici comuni con un'equazione di grado inferiore.—

3° Ogni funzione riducibile si può scindere in un sol modo in un prodotto di funzioni irriducibili.—

§ 58.— **Irriducibilità nel campo assoluto di razionalità.**— Sarà utile che, almeno nel caso speciale del campo assoluto di razionalità, dimostriamo la effettiva esistenza di funzioni irriducibili e diamo un procedimento per riconoscere sopra una funzione **data** se essa è o no riducibile.—

Una funzione razionale $f(x)$ nel campo assoluto [1] ha coefficienti razionali e moltiplicandola per un numero intero si può ridurre a coefficienti interi, sia

$$\varphi(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$

una tale funzione in cui i coefficienti a siano interi. Se m è il massimo comun divisore dei coefficienti a si dirà che m è il divisore della funzione $\varphi(x)$ (*) e la funzione stessa si dirà primitiva quando $m=1$. Cominciamo dal dimostrare il teorema di Gauss: Se le due funzioni $f(x)$, $\varphi(x)$ sono razionali intere a coefficienti interi e primitive, anche il loro prodotto $f(x)\varphi(x)$ sarà una funzione della medesima specie. È invero sia

$$f(x) = a_0 x^m + a_1 x^{m-1} + \dots + a_{m-1} x + a_m$$

$$\varphi(x) = b_0 x^n + b_1 x^{n-1} + \dots + b_{n-1} x + b_n$$

e

$$f(x)\varphi(x) = c_0 x^{m+n} + c_1 x^{m+n-1} + \dots + c_{m+n-1} x + c_{m+n}$$

dove

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 + a_1 b_0$$

(*) Se per la x in $\varphi(x)$ si pone un numero intero qualsiasi d, sarà $\varphi(d)$ un numero intero divisibile per m.

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$

e in generale

$$c_k = a_0 b_k + a_1 b_{k-1} + \dots + a_{k-1} b_1 + a_k b_0$$

coll' avvertenza che le a con indice superiore ad m come le b con indice superiore ad n sono nulle. Se la $f(x) \cdot \varphi(x)$ non fosse primitiva, esisterebbe almeno un fattore primo p comune a tutti i numeri c; ma siccome p non può, per ipotesi, dividere ne' tutte le a ne' tutte le b supponiamo che sia a_r il coefficiente a con indice più basso non divisibile per p, onde $r \leq m$ e così b_s il primo dei coefficienti b nella serie $b_0, b_1, \dots$ non divisibile per p e sarà $s \leq n$ (*).—

Costruendo il coefficiente

$$c_{r+s} = a_0 b_{r+s} + \dots + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + \dots + a_{r+s} b_0,$$

vediamo che nel secondo membro tutti i termini, tranne $a_r b_s$, sono divisibili per p e perciò c_{r+s} non è divisibile per p contro l' ipotesi.—

Dal teorema dimostrato segue come corollario:

(*) Naturalmente può anche darsi che uno dei due indici r, s sia zero ma non tutti e due perchè allora p non dividerebbe $c_0 = a_0 b_0$

Se le funzioni razionali intere a coefficienti interi $f(x)$, $\varphi(x)$ hanno i rispettivi divisori α, β sarà $\alpha\beta$ il divisore del loro prodotto $f(x)\varphi(x)$. — Abbiamo infatti

$$f(x) = \alpha f_1(x) \qquad \varphi(x) = \beta \varphi_1(x)$$

con f_1, φ_1 funzioni primitive e il prodotto $f(x)\varphi(x)$ che si ottiene moltiplicando la funzione primitiva $f_1(x)\cdot\varphi_1(x)$ per $\alpha\beta$ ha appunto per divisore $\alpha\beta$. — .

Possiamo altresì dimostrare che: Se una funzione $F(x)$ a coefficienti interi è riducibile, essa potrà scindersi nel prodotto di due altre funzioni a coefficienti interi. —

Basterà evidentemente dimostrare il teorema per una funzione primitiva $F(x)$. — Ora se si ha

$$F(x) = f(x)\varphi(x)$$

avendo f, φ coefficienti razionali, potremo moltiplicare per un conveniente numero intero N in modo da ottenere

$$N F(x) = f_1(x) \cdot \varphi_1(x)$$

ove f_1, φ_1 siano a coefficienti interi. Se la f_1 è a divisore α e la φ_1 a divisore β, per teorema dimostrato, essendo $F(x)$ primitivo, sarà $N = \alpha\beta$ e però troveremo

$$F(x) = \frac{f_1(x)}{\alpha} \cdot \frac{\varphi_1(x)}{\beta} \; . \qquad —$$

decomposta nel prodotto di due funzioni primitive.—
Dopo di ciò dimostriamo il teorema seguente che ci farà conoscere l'esistenza di infinite funzioni irriducibili di qualunque grado n:
Se p è un numero primo, la funzione intera a coefficienti interi

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots\cdots + a_{n-1} x + a_n$$

è certamente irriducibile se tutti i coefficienti, tranne il primo a_0, sono divisibili per p mentre l'ultimo a_n, che è divisibile per p non lo è per p^2.—
Supponiamo che $f(x)$ sia al contrario riducibile e però decomponibile nel prodotto di due funzioni

$$\varphi(x) = \alpha_0 x^r + \alpha_1 x^{r-1} + \cdots\cdots + \alpha_{r-1} x + \alpha_r$$

$$\psi(x) = \beta_0 x^s + \beta_1 x^{s-1} + \cdots\cdots + \beta_{s-1} x + \beta_s$$

a coefficienti α, β interi.— Sarà $r+s = n$ e

$$a_n = \alpha_r \beta_s$$

onde p dividerà uno ed uno solo dei due numeri α_r, β_s sia p. es. β_s.— Ora p non potendo dividere tutti i β, poichè altrimenti dividerebbe $a_0 = \alpha_0 \beta_0$, sia β_k il coefficiente β di massimo indice non divisibile per p, e però $0 \le k < s$. Il coefficiente a_{r+k} di x^{s-k} in $f(x)$ sarà dato da:

$$a_{r+k} = \alpha_r \beta_k + \alpha_{r-1} \beta_{k+1} + \alpha_{r-2} \beta_{k+2} + \ldots\ldots$$

e perciò non divisibile per p. perchè tutti i termini della somma del secondo membro tranne il primo, sono divisibili per p.

Vediamo in fine come dato una funzione $f(x)$ a coefficienti interi si possa riconoscere se essa è riducibile o no. Basterà evidentemente se $f(x)$ è di grado n, limitarsi a ricercarne i divisori razionali di grado $m \leq \frac{n}{2}$

Per trovare un tale divisore Kronecker fa uso del procedimento seguente (*). Essendo

$$z_0 \; z_1 \; z_2 \; \ldots\ldots \; z_n$$

$n+1$ numeri interi diversi ma del resto qualunque costruiamo le $n+1$ funzioni razionali di grado n

$$g_0(x) = \frac{(x-z_1)(x-z_2)\cdots(x-z_n)}{(z_0-z_1)(z_0-z_2)\cdots(z_0-z_n)} \quad , \quad g_1(x) = \frac{(x-z_0)(x-z_2)\ldots(x-z_n)}{(z_1-z_0)(z_1-z_2)\cdots(z_1-z_n)}$$

$$\ldots\ldots\ldots \quad g_n(x) = \frac{(x-z_0)(x-z_1)\cdots(x-z_{n-1})}{(z_n-z_0)(z_n-z_1)\cdots(z_n-z_{n-1})}$$

ostituite in guisa che si ha

$$g_i(z_k) = 0 \qquad \text{per } i \neq k$$

$$g_i(z_i) = 1$$

(*) Kronecker. – Grundzüge einer arithmetischen Theorie der algebraischen Grössen pag. 11. –

Ora essendo $\varphi(x)$ una funzione qualunque di grado $\underline{n}$, potremo esprimere linearmente ed omogeneamente $\varphi(x)$ per $g_0(x)\ g_1(x) \ldots\ldots g_n(x)$ colla formola

$$\varphi(x) = \varphi(z_0)\, g_0(x) + \varphi(z_1)\, g_1(x) + \ldots\ldots + \varphi(z_n)\, g_n(x),$$

giacchè i due polinomi nel primo e nel secondo membro, coincidendo per gli $n+1$ valori $z_0\ z_1 \ldots\ldots z_n$ della variabile x, coincidono assolutamente. Se dunque $\varphi(x)$ è un fattore di $f(x)$, nella decomposizione precedente dovrà essere $\varphi(z_i)$ un divisore dell'intero $f(z_i)$, onde, scritto i divisori diversi dei numeri

$$f(z_0)\quad f(z_1)\ \ldots\ldots\ f(z_n),$$

con un numero finito di tentativi potremo accertarsi se esiste un fattore $\varphi(x)$ di grado $\underline{n}$ e, nel caso affermativo determinarlo.—

133. Risolvente di Galois.— Sia

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots\ldots + a_{n-1} x + a_n = 0$$

una equazione che supporremo sempre **priva di radici multiple** (*) e indichiamo con $x_1\ x_2 \ldots\ldots x_n$ le

---

(*) È ben noto come alla risoluzione di un'equazione a radici multiple possa sostituirsi, con processi razionali, la ri-

sue radici. Consideriamo una funzione razionale (che possiamo sempre supporre intera) delle radici, sia

$$V = \varphi(x_1\, x_2 \cdots x_n) \ldots$$

Permutandovi le n radici nei $\pi(n)$ modi possibili la V acquisterà $\pi(n)$ valori che, scegliendo convenientemente la funzione φ, possiamo supporre distinti non solo **algebricamente** ma anche **numericamente**, come andiamo in primo luogo a dimostrare.. Prendiamo perciò semplicemente

$$V = \alpha_1 x_1 + \alpha_2 x_2 + \cdots\cdots + \alpha_n x_n$$

colle costanti α tutte diseguali fra loro; allora i $\pi(n)$ valori che assume V saranno certo **algebricamente** distinti, riguardando cioè $x_1, x_2 \ldots x_n$ come variabili indipendenti, ma potrà ben darsi che, avuto riguardo agli effettivi valori numerici delle radici, ve ne siano degli eguali. Tuttavia potremo sempre evitare questa eguaglianza **numerica** di due fra i $\pi(n)$ valori V nel modo seguente. Particolarizziamo ancora le costanti α assumendo $\alpha_1 = 1 \quad \alpha_2 = h, \ \alpha_3 = h^2 \ldots \alpha_{n-1} = h^{n-1}$;

l'eguaglianza numerica fra due valori della V:

$$x_{i_1} + h\, x_{i_2} + \cdots\cdots + h^{n-1} x_{i_n} = x_{\lambda_1} + h\, x_{\lambda_2} + \cdots + h^{n-1} x_{\lambda_n},$$

---

risoluzione di altrettante equazioni a radici semplici.—

denotando $(i, i_2 \ldots i_n)$, $(\lambda_1 \lambda_2 \ldots \lambda_n)$ due diverse permutazioni degli indici $1, 2, \ldots n$, porta che h debba soddisfare alla equazione non identica:

$$h^{n-1}(x_{i_n} - x_{\lambda_n}) + h^{n-2}(x_{i_{n-1}} - x_{\lambda_{n-1}}) + \ldots\ldots + (x_{i_1} - x_{\lambda_1}) = 0$$

Si vede dunque che soltanto per un numero **finito** di valori di h può aver luogo la detta eguaglianza numerica, che sarà dunque esclusa dando ad h un valore costante all'infuori di questi. — Ciò premesso e indicando con

$$s_1\ s_2 \ldots\ldots s_{\pi(n)}$$

le $\pi(n)$ sostituzioni sulle x, potremo indicare con V_{s_i} il valore che assume V effettuandosi sulle x la sostituzione s_i sicchè i $\pi(n)$ valori di V saranno

$$(a) \qquad V_{s_1}\ V_{s_2} \ldots\ldots V_{s_{\pi(n)}}$$

e inversamente a ciascuno di questi valori corrisponderà una ed una sola sostituzione. — Ora, essendo y una variabile, costruiamo il polinomio di grado $\pi(n)$ in y

$$(b) \qquad \psi(y) = (y - V_{s_1})(y - V_{s_2}) \cdot \ldots\ldots (y - V_{s_{\pi(n)}});$$

i suoi coefficienti sono le funzioni simmetriche elementari dei $\pi(n)$ valori V e quindi, come è chiaro, essi sono funzioni simmetriche delle radici della proposta, esprimibili per ciò razionalmente per i coefficienti di questa. Avremo dunque $\psi(y) = y^{\pi(n)} + \beta_1 y^{\pi(n)-1} + \beta_2 y^{\pi(n)-2} + \ldots + \beta_{\pi(n)}$,

i coefficienti β essendo razionalmente noti. La equazione $\psi(V)=0$, che ha manifestamente per radici le $\pi(n)$ quantità distinte (a), dicesi risolvente di Galois della equazione data.(*)

Dimostriamo ora il seguente teorema fondamentale:
Qualunque funzione razionale $\mathfrak{F}(x_1 x_2 \dots x_n)$ delle radici della proposta è razionalmente esprimibile per una qualunque radice della risolvente di Galois, per es. per $V_{j_1} = V_1$

Denotando con

$$\mathfrak{F}_{j_1}\ \mathfrak{F}_{j_2}\ \dots\dots\ \mathfrak{F}_{j_{\pi(n)}}$$

i valori che assume $\mathfrak{F}(x_1 x_2 \dots x_n)$ permutandovi le x_1, valori che potranno essere anche tutti distinti ed avendo $\psi(V)$ il significato della (b), consideriamo la funzionale razionale intera della V di grado $\pi(n)-1$ data da

---

(*) È chiaro che la costruzione di questa risolvente per mezzo della funzione $V = x_1 + h x_2 + \dots\dots + h^{n-1} x_n$, ove si lasci h indeterminato, da modo di scegliere poi per h un valore conveniente sì che la risolvente stessa non abbia radici eguali, ciò che si ottiene dando ad h un valore che non ne annulli il discriminante.

$$\Phi(y)=\left\{\frac{\mathfrak{I}_{s_1}}{y-V_{s_1}}+\frac{\mathfrak{I}_{s_2}}{y-V_{s_2}}+\cdots\cdots+\frac{\mathfrak{I}_{s_{\pi(n)}}}{y-V_{s_{\pi(n)}}}\right\}\psi(y)$$

i coefficienti della $\Phi(y)$ sono funzioni simmetriche delle $x_1\ x_2\ \ldots\ x_n$ e per ciò razionalmente note. - Facendo nella precedente $y=V_{s_i}$ otteniamo

$$\Phi(V_{s_i})=\mathfrak{I}_{s_i}\cdot\psi'(V_{s_i})$$

indicando ψ' il polinomio derivato di ψ; abbiamo dunque (essendo $\psi'(V_{s_i})\neq 0$)

$$\mathfrak{I}_{s_i}=\frac{\Phi(V_{s_i})}{\psi'(V_{s_i})}\ ,$$

alla quale formola, facendo uso della

$$\psi(V_{s_i})=0$$

possiamo dare, come è ben noto, la forma

$$(c)\qquad \mathfrak{I}_{s_i}=\Theta(V_{s_i})\ ,$$

essendo Θ una funzione razionale intera del suo argomento di grado non superiore a $\pi(n)-1$, indipendente affatto dall'indice i della V_{s_i}, e con coefficienti razionali. - Abbiamo dunque in particolare, come si voleva

$$\mathfrak{I}(x_1\cdots x_n)\,\mathfrak{I}_{s_1}=\Theta(V_{s_1})$$

e di più vediamo, ciò che è molto importante per il seguito: Nella formola $\mathfrak{I}(x_1x_2\cdots x_n)=\Theta(V_{s_1})$ che esprime una funzione razionale delle radici della

proposta razionalmente per una radice V_1 della risolvente di Galois è lecito fare qualsiasi sostituzione sulle x ed essa rimane sempre vera.-

§ 60.- Proprietà della risolvente di Galois.-

La proprietà fondamentale ora dimostrata da luogo a diverse conseguenze che importa notare. In primo luogo se per $\mathcal{F}(x_1 x_2 \ldots x_n)$ si prende una qualunque delle radici della proposta si vede che: Ogni radice della proposta è razionalmente esprimibile per una radice arbitraria della risolvente di Galois.- Basterebbe dunque conoscere una radice di questa risolvente per conoscere tutte le radici della proposta, che sarebbe allora risoluta.

Se prendiamo poi per $\mathcal{F}$ una qualunque delle altre radici della risolvente stessa, veniamo che: La risolvente di Galois gode della proprietà che, fissata una sua radice qualunque, tutte le altre radici possono esprimersi razionalmente per questa.-

Si vede anche che due diverse risolventi di Galois della proposta si ottengono l'una dall'altra con una sostituzione di Tschirnhaus; noi le riguardiamo

perciò come essenzialmente identiche e parleremo quindi della risolvente di Galois, intendendo di assumerla sotto una qualunque delle sue forme.

La risolvente di Galois, che non ha certamente radici eguali, può essere riducibile o no. In particolare essa può essere riducibile sia nel campo di razionalità determinato dai coefficienti della primitiva, sia perché coll'aggiunta di nuove quantità si è ampliato il campo di razionalità. In ogni caso però diciamo che sussiste il teorema:

Se la risolvente di Galois è riducibile i fattori irriducibili in cui si spezza sono tutti di egual grado.

Benché la dimostrazione di questa proprietà risulti anche indirettamente dai seguenti §§, non sarà inutile darne una dimostrazione diretta fondata sulla proprietà fondamentale della risolvente di Galois che ogni radice è razionalmente esprimibile per qualsiasi altra.

Basterà evidentemente dimostrare che se

$$\varphi(y) = (y - V_1)(y - V_2) \cdots (y - V_r)$$

è un fattore irriducibile di grado r di $\psi(V)$, nessun

altro fattore potrà avere un grado maggiore. Sia $\varphi_1(y)$ un altro fattore irriducibile e V_i una sua radice; sarà

$$V_i = \theta(V_1),$$

essendo θ razionale intera in V_1. Poichè

$$\varphi_1(V_i) = \varphi_1\big(\theta(V_1)\big) = 0$$

l'equazione

$$\varphi_1\big(\theta(y)\big) = 0$$

ammette la radice V_1 dell'equazione irriducibile $\varphi(y) = 0$ e però tutte, onde

$$\theta(V_1) \quad \theta(V_2) \cdots\cdots \theta(V_z)$$

sono altrettante radici di $\varphi_1(y) = 0$. Ora nel polinomio

$$[y - \theta(V_1)][y - \theta(V_2)] \cdots\cdots [y - \theta(V_z)]$$

che è un fattore di $\varphi_1(y)$, i coefficienti sono funzioni simmetriche delle radici $V_1, V_2 \cdots V_z$ di $\varphi(y) = 0$ e però razionalmente noti; è quindi impossibile che il grado del fattore irriducibile $\varphi_1(y)$ superi z.

In generale chiameremo **equazioni normali** quelle per le quali, fissata ad arbitrio una radice, tutte le altre sono esprimibili razionalmente per questa e potremo dunque enunciare il resultato: Se un'equazione normale è riducibile, essa si spezza in altrettante equazioni normali irriducibili tutte di egual grado.

§61. — **Gruppo di Galois per l'equazione.** — Consideriamo un fattore irriducibile $\varphi(y)$ della risolvente di Galois p. es. quello che contiene la prima radice V_{s_1} e siano (d) $V_{s_1}\ V_{s_2}\ V_{s_3} \cdots \cdots V_{s_r}$ le sue r radici. — Dimostriamo che: Le r sostituzioni sulle x $\quad s_1, s_2 \ldots s_r,$ colle quali si passa dalla prima alle altre radici del fattore irriducibile considerato della risolvente di Galois, formano un gruppo. —

La dimostrazione resulta subito da quanto si è visto al §59 formola (c). — È invero essendo V_{s_i} una qualunque delle radici (d) sarà

$$V_{s_i} = \Theta(V_{s_1})$$

essendo Θ razionale intera in V_{s_1} e siccome in una tale sostituzione è lecita (§ 59) qualunque sostituzione sulle x operazioni la s_k $(k = 1, 2, \cdots r)$ avremo

$$(e) \qquad V_{s_i s_k} = \Theta(V_{s_k})$$

Ma si ha

$$\varphi(V_{s_i}) = \varphi[\Theta(V_{s_1})] = 0$$

cioè

$$\varphi[\Theta(y)] = 0$$

ha la radice V_{s_1} della equazione irriducibile $\varphi(y) = 0$ quindi anche le altre, in particolare V_{s_k} onde $\varphi[\Theta(V_{s_k})] = 0$ cioè per la (e)

$$\varphi(V_{s_i s_k}) = 0$$

Dunque $V_{s_i s_k}$ è eguale ad una delle (d) cioè

$$s_i s_k = s_l \qquad (l \leq r),$$

ciò che dimostra appunto il teorema enunciato.—

Ora se distribuiamo le $\pi(n)$ sostituzioni sulle radici x rispetto al gruppo $\mathfrak{S}_r = (s_1 s_2 \ldots\ldots s_r)$ nel quadro

s_1 ,	s_2		s_r
$t_2 s_1$,	$t_2 s_2$		$t_2 s_r$
. . . . .			
$t_q s_1$,	$t_q s_2$		$t_q s_r$

vediamo subito, colle considerazioni del § 60, che le radici V della risolvente di Galois aventi per indici le sostituzioni di una stessa orizzontale nel quadro appartengono ad un medesimo fattore irriducibile.— E infatti sia p.es. $\varphi_1(y)$ il fattore irriducibile che contiene la radice V_{i_2}; avremo

$$V_{t_2} = \Theta(V_{s_1}),$$

essendo Θ razionale intera nel suo argomento e di qui deduciamo

$$V_{t_2 s_i} = \Theta(V_{s_i})$$

Ora da $\varphi_1(V_{t_2}) = \varphi_1[\Theta(V_{s_1})] = 0$ deduceni nel solito modo

$$\varphi_1[\Theta(V_{s_i})] = \varphi_1(V_{t_2 s_i}) = 0,$$

onde risulta appunto che tutte le radici $V_{t_2 s_i}$ $(i = 1, 2 \cdots r)$

appartengono ad uno stesso fattore irriducibile. Si vede quindi che da qualunque fattore irriducibile della risolvente di Galois si porta le sostituzioni sulle x, che fanno passare dall'una all'altra delle sue radici, formano sempre il medesimo gruppo. Esso dicesi il gruppo di Galois per l'equazione.

Osserviamo che essendo le n radici della proposta funzioni razionali intere di V_{s_1}, potremo scrivere

$$x_1 = \Theta_1(V_{s_1}) \quad x_2 = \Theta_2(V_{s_1}) \cdots\cdots\cdots x_n = \Theta_n(V_{s_1})$$

e per l'osservazione fondamentale alla fine del § 59 una qualunque di queste relazioni rimane vera effettuandosi qualunque sostituzione sulle x, in particolare una s_k del gruppo di Galois, sicchè

$$\Theta_1(V_{s_k}) \quad \Theta_2(V_{s_k}) \cdots\cdots\cdots \Theta_n(V_{s_k})$$

sono le radici stesse $x_1\ x_2 \ldots x_n$ permutate nel modo assegnato dalla s_k. Possiamo dunque ottenere il gruppo di Galois anche nel modo seguente: Si esprimano le n radici x della proposta razionalmente per una radice della risolvente di Galois; cangiando in queste espressioni quella radice in tutte le altre, appartenenti al medesimo fattore irriducibile della risolvente, le n radici x si permutano fra loro

appunto secondo le sostituzioni del gruppo di Galois.

§ 62. **Proprietà caratteristiche del gruppo di Galois.** — Passiamo ora a dimostrare i teoremi fondamentali relativi al gruppo di Galois per l'equazione $f(x) = 0$.

I) Se una funzione razionale $\mathfrak{F}(x_1 x_2 \ldots x_n)$ delle n radici di $f(x) = 0$ rimane **numericamente** invariata per qualsiasi sostituzione del gruppo di Galois, essa è razionalmente nota.

Indicando con $\mathfrak{F}_{s_i}$ il valore che assume $\mathfrak{F}$ con la sostituzione s_i del gruppo di Galois effettuata sulla x, si ha per ipotesi

$$\mathfrak{F}_{s_1} = \mathfrak{F}_{s_2} = \mathfrak{F}_{s_3} = \ldots\ldots\ldots = \mathfrak{F}_{s_r}$$

Ora si ha (§ 59)

$$\mathfrak{F}_{s_i} = \Theta(V_{s_i})$$

designando Θ una funzione razionale intera e perciò il valore numerico di $\mathfrak{F}(x_1 x_2 \ldots x_n)$ può anche esprimersi con

$$\mathfrak{F}(x_1 x_2 \ldots x_n) = \frac{1}{r}\left\{\Theta(V_{s_1}) + \Theta(V_{s_2}) + \ldots + \Theta(V_{s_r})\right\}$$

Il secondo membro essendo una funzione simmetrica delle radici del primo fattore irriducibile della risolvente di Galois ap-

partiene al campo attuale di razionalità c. d. d.

Inversamente dimostriamo:

II) Se una funzione razionale della radice di $f(x)=0$, sia $\mathcal{F}(x_1\, x_2 \cdots x_n)$, è razionalmente nota, il suo valore numerico non cangia effettuando sulle x qualunque sostituzione del gruppo di Galois.—

Sia infatti $\mathcal{F}(x_1\, x_2 \cdots x_n) = A$

la quantità A appartenendo al campo attuale di razionalità $(R, R', R'' \ldots)$. Possiamo esprimere $\mathcal{F}(x_1 x_2 \cdots x_n)$ per una funzione razionale intera $\Theta(V_{s_1})$ di V_{s_1} onde avremo

$$\Theta(V_{s_1}) - A = 0,$$

cioè l'equazione $\Theta(y) - A = 0$ ammette la radice V_{s_1} e quindi tutte le altre del primo fattore irriducibile, quindi $\Theta(V_{s_1}) = \Theta(V_{s_2}) = \cdots\cdots\cdots = \Theta(V_{s_2}) = A$

Ma si ha $\mathcal{F}_{s_i} = \Theta(V_{s_i})$ (§ 59) e però

$$\mathcal{F}_{s_1} = \mathcal{F}_{s_2} = \mathcal{F}_{s_3} = \cdots\cdots\cdots = \mathcal{F}_{s_2} \quad \text{c. d. d.}$$

Oss.ne — Segue di qui che se due funzioni razionali delle radici $\mathcal{F}(x_1\, x_2 \cdots x_n)$, $\Phi(x_1\, x_2 \cdots x_n)$ hanno il medesimo valore numerico $\mathcal{F}(x_1 x_2 \cdots x_n) = \Phi(x_1 x_2 \cdots x_n)$

sarà anche $\mathcal{F}_{s_i} = \Phi_{s_i}$

poichè la differenza $\mathcal{F}(x_1 x_2 \cdots x_n) - \Phi(x_1 x_2 \cdots x_n)$ essendo

razionalmente nota = 0, essa resterà ancora nulla eseguendo qualunque sostituzione del gruppo di Galois. Ma non sarebbe lecito concludere

$$\mathfrak{F}_U = \Phi_U ,$$

se la sostituzione U non appartiene al gruppo di Galois. Le proprietà del gruppo di Galois superiormente dimostrate sono caratteristiche per le sostituzioni di questo gruppo, come resulta dal teorema seguente:

III) **Nessuna sostituzione, all'infuori di quelle del gruppo di Galois, può lasciare invariata qualsiasi funzione razionale delle radici razionalmente nota.**

Essendo infatti S un'indeterminata appartenente al campo di razionalità, la funzione razionale delle radici

$$\mathfrak{F} = (S - V_{s_1})(S - V_{s_2}) \cdot \cdots \cdot (S - V_{s_n}) = \Psi(S)$$

è razionalmente nota; ma una sostituzione U fuori del gruppo di Galois la cangia in

$$\mathfrak{F}_U = (S - V_{s_1 U})(S - V_{s_2 U}) \cdot \cdots \cdot (S - V_{s_n U})$$

che può avere il valore numerico precedente solo per un numero finito di valori di S che possiamo sempre evitare. — Risulta di qui che se per un'equazione data riusciamo a trovare un gruppo T di sostituzioni sulle radici tale che

ogni sostituzione di T lasci numericamente invariate tutte le funzioni razionali delle radici razionalmente note, il gruppo T coinciderà col gruppo di Galois ovvero sarà un suo sottogruppo.-

§ 63.- **Riduzione del gruppo di Galois per aggiunta di quantità**.- Il gruppo di Galois per una equazione $f(x)=0$ è essenzialmente relativo al campo di razionalità $(R, R', R'' \ldots)$ attuale.- Se il campo si amplia per **aggiunta** di nuove quantità (§ 57), può accadere naturalmente che il gruppo di Galois cangi; in ogni caso vediamo subito: **Ampliando il campo di razionalità il gruppo di Galois rimarrà lo stesso, ovvero si ridurrà ad un suo sottogruppo**.- È invero se il primitivo fattore irriducibile

$$(y - V_{s_1})(y - V_{s_2}) \cdots (y - V_{s_2})$$

della risolvente di Galois rimane irriducibile anche nel nuovo campo, il gruppo rimane evidentemente lo stesso; se il fattore stesso diventa riducibile, sia

$$(y - V_{s_1})(y - V_{s_2}) \cdots (y - V_{s_i})$$

un suo fattore irriducibile sarà

$$T_i = (s_1 s_2 \cdots s_i)$$

il nuovo gruppo di Galois, che è dunque un sottogruppo del primitivo.

Ciò premesso osserviamo che se $F(x_1, x_2 \ldots x_n)$ è una funzione ovunque razionale delle radici di $f(x) = 0$: Quelle sostituzioni del gruppo G_x di Galois che lasciano numericamente invariata $F(x_1, x_2 \cdots x_n)$ formano in G_x un sottogruppo. — È infatti se s_i, s_k sono due tali sostituzioni di G_x avremo

$$F_{s_i} = F_{s_1} \quad , \quad F_{s_k} = F_{s_1} \qquad (s_1 = 1)$$

e quindi, per l'osservazione fatta nel § precedente

$$F_{s_i s_k} = F_{s_k} = F(x_1, x_2 \cdots x_n)$$

cioè anche il prodotto $s_i s_k$ lascia F numericamente invariata (*). —

(*) È bene osservare con Holder (Math. Annalen Bd. 34) che la stessa proprietà non vale più per sostituzioni che siano fuori del gruppo di Galois. — Così p.es. se prendiamo l'equazione

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$$

le cui n radici sono $x_z = e^{\frac{2\pi i z}{n}}$ $(z = 1, 2, \cdots n-1)$ e prendiamo il prodotto $x_1 x_{n-1} = 1$ le due sostituzioni $(x_1 x_2)(x_{n-1} x_{n-2})$, $(x_1 x_{n-1})(x_2 x_3)$ lo lasciano numericamente invariato, ma se $n > 5$, il loro prodotto lo cangia in $x_3 x_{n-2}$ che non è più $= 1$.

Ora dimostriamo il teorema: Se si amplia il campo di razionalità aggiungendovi una funzione razionale $z_1 = F(x_1 x_2 \dots x_n)$ delle radici il gruppo di Galois G_x si abbasserà a quel suo sottogruppo T le cui sostituzioni lasciano numericamente invariata la funzione aggiunta.—

Che il nuovo gruppo contenga soltanto sostituzioni di T risulta evidente dall'osservare che, essendo $z_1 = F(x_1 x_2 \dots x_n)$ razionale nel nuovo campo, le sostituzioni del nuovo gruppo di Galois debbono lasciarla numericamente invariata. Per dimostrare poi che qualsiasi sostituzione s di T appartiene al nuovo gruppo di Galois basterà (pel § 62 III)) dimostrare che s lascia invariata ogni funzione razionale delle radici razionalmente nota nel nuovo campo. Per una tale funzione $\Psi(x_1 x_2 \dots x_n)$ dovrà invero infatti

$$\Psi(x_1 x_2 \dots x_n) = \Theta(z_1)$$

ove Θ è razionale in z_1 con coefficienti appartenenti all'antico campo di razionalità. — Eseguendo nella relazione precedente la sostituzione s dell'antico gruppo di Galois ne deduciamo

$$\Psi_s = \Theta(z_s)$$

poichè $z_s = z_1$ sarà anche

$$\Psi_s = \Psi(x_1 x_2 \dots x_n) \qquad \text{c. d. d.}$$

§64. – **Transitività od intransitività del gruppo di Galois.** – Vedremo in seguito come tutte le proprietà dei gruppi che abbiamo studiato nella prima parte si traducano, colla nozione del gruppo di Galois per una equazione, in altrettante proprietà della equazione stessa. – Qui cominciamo dal dimostrare il seguente importante teorema:

Un' equazione $f(x)=0$ è riducibile od irriducibile secondo che il suo gruppo di Galois è intransitivo ovvero transitivo. –

Supponiamo il gruppo di Galois G_r intransitivo. – Le n radici $x_1\, x_2 \ldots x_n$ si scindono allora in sistemi di transitività tali che le radici di ciascun sistema sono scambiate fra loro transitivamente dalle sostituzioni di G_r ($P^a I^a$ §9). –

Sia
$$x_1, x_2, \ldots x_i \qquad (i < \pi)$$
un tale sistema; il fattore di $f(x)$
$$(x-x_1)(x-x_2)\ldots\ldots(x-x_i)$$
è razionalmente noto perchè le sostituzioni del gruppo di Galois, scambiando fra loro $x_1\, x_2 \ldots x_i$, lo lasciano numericamente invariato, onde segue che $f(x)=0$ è riducibile.

Dunque se $f(x)=0$ è irriducibile, il gruppo di Galois è necessariamente transitivo. –

Basterà ora evidentemente dimostrare che se $f(x)=0$ è ridu-

ibile il gruppo G_2 è intransitivo, onde seguirà che se G_2 è transitivo sarà $f(x)=0$ irriducibile. Ora se

$$(x-x_1)(x-x_2)\dots(x-x_i)$$

è un fattore razionalmente noto di $f(x)$, le sostituzioni di G_2 dovendo lasciarlo numericamente invariato (qualunque sia x) non potranno che scambiare fra loro $x_1\ x_2 \dots x_i$ e però G_2 sarà intransitivo c. d. d.

§65. Equazioni che hanno per gruppi di Galois il gruppo totale.

Denotiamo con

$$f(x)= x^n + c_1 x^{n-1} + c_2 x^{n-2} + \dots + c_{n-1}x + c_n = 0$$

l'equazione generale di grado n dove dunque i coefficienti c restano indeterminati. Quale sarà il gruppo di Galois dell'equazione $f(x)=0$ nel campo di razionalità $(c_1\ c_2\ c_3 \dots c_n)$? È facile vedere che tale gruppo è il gruppo totale $G_{\pi(n)}$ sulle n radici. Ammesso infatti che ne fosse un sottogruppo $G_2 = (s_1\ s_2 \dots s_2)$ indicando con $V_{s_1}\ V_{s_2} \dots V_{s_2}$ le radici del primo fattore irriducibile della risolvente di Galois, una funzione simmetrica di queste p. es.

$$F(x_1\ x_2 \dots x_n) = V_{s_1} + V_{s_2} + \dots + V_{s_2}$$

che è funzione non simmetrica delle radici di $f(x)=0$

sarebbe razionalmente esprimibile per $c_1\, c_2 \ldots c_n$ ed eguale quindi ad una funzione simmetrica $\Phi(x_1 x_2 \ldots x_n)$ delle radici stesse.-

Una tale eguaglianza

$$F(x_1 x_2 \ldots x_n) = \Phi(x_1 x_2 \cdots x_n)$$

restando indeterminate le c quindi le x stesse, è evidentemente assurda.

Ma si può dimostrare di più che si possono trovare anche equazioni con coefficienti numerici che hanno per gruppo il gruppo totale.-

Da alcuni teoremi generali sulle funzioni a più variabili irriducibili Hilbert (*) ha dedotto in particolare il teorema: Si possono costruire infinite equazioni, di grado dato n, con coefficienti numeri interi, che nel campo assoluto di razionalità hanno per gruppo di Galois il gruppo totale.-

Noi qui ci contenteremo di riportare la dimostrazione data dal Weber (**) pel caso in cui n è un numero primo.- Costruiamo per ciò, e col processo del § 58, n

---

(*) Journal von Crelle T.° 110

(**) Lehrbuch der Algebra T. I pag. 605

na equazione irriducibile

$$\varphi(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0 \quad ,$$

i cui coefficienti siano numeri interi e supponiamo che il suo gruppo di Galois G_r non coincida col gruppo totale. — G_r è certamente transitivo, l'equazione essendo irriducibile, e per il resultato in fine al § 13 P.te I.a non può contenere alcuna trasposizione. — Se ora aggiungiamo al campo di razionalità $n-2$ delle radici di $f(x)=0$, pel teorema al § 63, il gruppo di Galois scenderà a quel suo sottogruppo che le lascia tutte singolarmente invariate cioè, per quanto precede, all'identità; dunque le altre due radici saranno pure razionalmente note. — Ne segue che se un'equazione irriducibile di grado primo n, a coefficienti numerici ha per gruppo di Galois un gruppo inferiore al gruppo totale e se $n-2$ delle sue radici sono reali anche le altre due saranno reali. — Dunque:

Un'equazione irriducibile di grado primo n con coefficienti interi, che abbia $n-2$ radici reali e due immaginarie, avrà per gruppo di Galois il gruppo totale. —

Basterà dunque far vedere come si può effettivamente costruire infinite equazioni di questa specie. —

Si prenda per ciò un'equazione a coefficienti reali

$$x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \ldots + \alpha_{n-1} x + \alpha_n = 0$$

con $n-2$ radici reali e due immaginarie. – Facendo variare sufficientemente poco i coefficienti α, variano anche di tanto poco quanto si vuole le radici, in particolare $n-2$ restano reali e due immaginarie. – Ora possiamo prendere in infiniti modi i coefficienti interi

$$a_0 \quad a_1 \quad a_2 \ldots\ldots a_n$$

della $\varphi(x)$ in guisa che a_0 non sia divisibile per p, e invece $a_1 a_2 \ldots a_n$ divisibili ma però a_n non divisibile per p^2 e inoltre che le frazioni

$$\frac{a_1}{a_0} \quad \frac{a_2}{a_0} \ldots\ldots \frac{a_n}{a_0}$$

siano vicine quanto si vuole rispettivamente ad

$$\alpha_1 \quad \alpha_2 \ldots\ldots \alpha_n \; .$$

Così otterremo quante si vogliano equazioni irriducibili

$$\varphi(x) = a_0 x^n + \ldots\ldots + a_n = 0$$

a coefficienti interi con $n-2$ radici reali e 2 immaginarie, che avranno quindi per gruppo nel campo assoluto di razionalità, il gruppo totale. –

Così p. es. l'equazione di 5° grado irriducibile

$$x^5 + 5x^2 - 5x - 5 = 0$$

ha tre radici reali, una positiva, due negative e le al

le due immaginarie, onde il suo gruppo sarà il gruppo totale sulle cinque radici.–

§ 66.– Formazione generale delle risolventi.

– Prendiamo una funzione razionale qualunque

$$y_1 = \psi(x_1, x_2 \ldots x_n)$$

delle radici della proposta.– Quelle sostituzioni del gruppo $\mathfrak{G}_2$ di Galois che lasciano y_1 numericamente invariata formano, come abbiamo visto al § 63, un sottogruppo di $\mathfrak{G}_2$; sia questo sottogruppo

$$T_\delta = (1, s_2 \ldots s_\delta)$$

che diremo il **sottogruppo numerico** della y_1. Indicando con q l'indice di T_δ in $\mathfrak{G}_2$ poniamo nel solito modo

$$\mathfrak{G}_2 = (T_\delta, T_\delta t_2, \ldots T_\delta t_q)$$

Essendo y_σ il valore che assume y_1 dopo la sostituzione σ del gruppo di Galois effettuata sulle x si vede subito che sarà

$$y_\sigma = y_{\sigma'} \quad (*)$$

solo quando σ, σ' sono equivalenti rispetto al sot-

(*) Da $y_{\sigma'} - y_\sigma = 0$ applicando la σ^{-1} del gruppo di Galois segue $y_{\sigma'\sigma^{-1}} = y_1$ onde $\sigma'\sigma^{-1} = s_i$.–

sottogruppo T nel senso del § 24. — I valori distinti che assume y_1 per le sostituzioni di G_2 sono dunque soltanto

$$(\gamma) \qquad y_1 \; y_{t_2} \; \ldots\ldots \; y_{t_q}$$

e se effettuiamo contemporaneamente destro queste q γ una sostituzione del gruppo di Galois G, esse si permutano fra loro precisamente secondo la corrispondente sostituzione del gruppo complementare $\frac{G}{T}$ (§ 24). — Se ora costruiamo il polinomio razionale intero di grado q nella variabile y:

$$\Phi(y) = (y - y_1)(y - y_{t_2})(y - y_{t_3}) \ldots\ldots (y - y_{t_q})$$

i suoi coefficienti come funzioni simmetriche delle q funzioni (γ), che le sostituzioni di G_2 permutano fra loro, saranno razionalmente noti. —

L'equazione $$\Phi(y) = 0$$

che si può costruire razionalmente ed ha per radici i valori che assume la funzione $y_1 = \psi(x_1, x_2 \ldots x_n)$ [illegible] le sostituzioni del gruppo di Galois, dicesi una **risolvente** della proposta. — Se si aggiunge al campo di razionalità la prima radice y_1 della risolvente $\Phi(y) = 0$, il gruppo di Galois scende da G a T (§ 23) e più in [illegible] funzione razionale z_1 delle radici della proposta il cui sottogruppo rimanga lo stesso T [illegible]

sonalmente nota. - Ne risulta che se costruiamo due diverse risolventi con due funzioni y_1, z_1 aventi lo stesso gruppo numerico T; esse saranno trasformate di Tschirnhaus l'una dell'altra e noi le riguarderemo come identiche. - Ora vediamo facilmente che: scelto ad arbitrio un sottogruppo T del gruppo G di Galois, potremo sempre costruire una funzione razionale delle radici della proposta che abbia per gruppo numerico precisamente

$$T = (j_1\, j_2 \ldots\ldots j_m).$$

È invero, indicando al solito con V_{y_i} le radici del primo fattore irriducibile della risolvente di Galois pongasi

$$y_1 = (S - V_{y_1})(S - V_{y_2}) \ldots\ldots (S - V_{y_m})$$

ove S è un'indeterminata qualunque nel campo di razionalità. Per qualunque sostituzione di T la y_1 rimane invariata, per un'altra sostituzione g di G essa diventa $(S - V_{y_1 g})(S - V_{y_2 g}) \ldots\ldots (S - V_{y_m g})$;
questo valore non è <u>identicamente</u> eguale al precedente e possiamo quindi sempre evitare quei particolari valori di S per i quali avrebbe luogo una tale eguaglianza. - Così la y_1 avrà appunto per sottogruppo numerico T. -

§ 67. - **Gruppo della risolvente.** - Ritornando alla ri-

solvente generale $\Phi(y)=0$ colle q radici (1), domandiamo: Quale è il gruppo di Galois per la risolvente? — Abbiamo già detto che eseguendo dentro le funzioni

$$(2) \qquad y_{t_1},\ y_{t_2} \cdots y_{t_q},$$

che sono le q radici della risolvente, le sostituzioni del gruppo di Galois sulle x, esse si permutano fra loro secondo le sostituzioni del gruppo complementare $H=\frac{G}{T}$ di G rispetto a T. — Ne segue facilmente: La risolvente costruita con una funzione y_1 razionale delle radici della proposta, a gruppo numerico T, ha precisamente per gruppo di Galois il gruppo complementare $H=\frac{G}{T}$ del gruppo della proposta rispetto al sottogruppo T. —

È infatti una funzione razionale

$$\mathcal{U}(y_{t_1}, y_{t_2} \ldots y_{t_q})$$

delle q radici della risolvente è una funzione razionale delle x, sia

$$\mathcal{U}(y_{t_1}, y_{t_2} \cdots y_{t_q}) = F(x_1 x_2 \cdots x_n)$$

Le sostituzioni di G eseguite sulle x producono sulle y le sostituzioni di H; ne segue che se $\mathcal{U}$ è razionalmente nota deve restare numericamente invariata per tutte

le sostituzioni di H e viceversa, se ciò accade, essa è razionalmente nota.- Dunque H è precisamente il gruppo di Galois per la risolvente $\Phi(y)=0$.- Evidentemente H è transitivo e perciò le risolventi costruite nel modo che abbiamo detto sono sempre irriducibili.-

Cerchiamo ora quale vantaggio si sarà ottenuto per la risoluzione della proposta quando la risolvente $\Psi(y)=0$ sia risolta, cioè tutte le sue radici siano aggiunte al campo di razionalità.- Pel teorema fondamentale al §63 il gruppo di Galois per la proposta si abbassava allora a quel sottogruppo Σ, che lascia singolarmente invariato il valore numerico di ciascuna radice della risolvente, cioè a quelle sostituzioni di G che corrispondono all'identità in H.(*) In ogni caso Σ è un sottogruppo invariante in G, talchè se G è semplice, Σ sarà G stesso o l'identità.- In quest'ultimo caso col-

---

(*) Ciò si vede anche subito osservando che essendo T il sottogruppo numerico di y_1 sarà

$$T' = E' T E$$

quello di y_t perchè da $y_{t\sigma} - y_t = 0$ segue $y_{t\sigma t'} = y_1$ cioè

$t\sigma E' = \gamma$, $\sigma = E' \gamma E$.-

la risoluzione della risolvente è già ottenuta anche quella della proposta, ma il gruppo della $\Phi(y)=0$ è olodricamente isomorfo con quello di $f(x)=0$

§68.— Equazioni a gruppo imprimitivo.— Abbiamo esaminato al §64 a quale proprietà della equazione corrisponde la transitività od intransitività del gruppo, vediamo ora quale proprietà speciale appartiene ad un'equazione il cui gruppo $\mathfrak{S}$ di Galois sia imprimitivo. Se le n radici di $f(x)=0$ si tendono in r sistemi d'imprimitività contenenti ciascuno s radici talchè $n=rs$, distingueremo per comodità le radici con un doppio indice di cui il primo si riferisce al sistema d'imprimitività, il secondo al posto che vi occupa la radice. Così distribuiamo le n radici nel quadro:

$$\begin{Vmatrix} x_{11} & x_{12} & \dots & x_{1s} \\ x_{21} & x_{22} & \dots & x_{2s} \\ \dots & \dots & \dots & \dots \\ x_{r1} & x_{r2} & \dots & x_{rs} \end{Vmatrix}$$

le cui orizzontali rappresentano i sistemi d'imprimitività.— Prendiamo ora una funzione simmetrica delle radici della prima orizzontale p. es. $y_1=(S-x_{11})(S-x_{12})\dots\dots(S-x_{1s})$

I valori distinti che assumerà

$$y_1 = F(x_{11}\ x_{12} \ldots\ldots x_{1s})$$

saranno al più r

$$y_i = F(x_{i1}\ x_{i2} \ldots x_{is}) \quad i = 1, 2 \ldots r$$

e noi supponiamo appunto y_1 presa in modo che questi r valori siano numericamente distinti, ciò che è sempre possibile (*). - Costruiamo la risolvente

$$\Phi(y) = (y-y_1)(y-y_2)\ldots\ldots(y-y_r) = 0$$

che avrà precisamente per gruppo il gruppo indotto da G sui sistemi d' imprimitività. - Se aggiungiamo al campo di razionalità la radice y_1 della $\Phi(y)=0$ il gruppo G si abbassa a quel sottogruppo che lascia fermo il primo sistema d' imprimitività e però il fattore della proposta

$$(x-x_{11})(x-x_{12})\ldots\ldots(x-x_{1s})$$

né viene separato razionalmente e si ha dunque

$$(x-x_{11})(x-x_{12})\ldots(x-x_{1s}) = x^s + \alpha_1(y_1)x^{s-1} + \alpha_2(y_1)x^{s-2} + \ldots\ldots + \alpha_s(y_1),$$

dove le α sono razionali intere in y_1 con coefficienti appartenenti all'antico campo di razionalità. - Eseguendo sulla identità precedente una sostituzione di G che porti il primo sistema di imprimitività nell' i^{mo} avremo:

(*) Basta al solito evitare particolari valori di p. -

$$(x-x_{i_1})(x-x_{i_2})\ldots\ldots(x-x_{i_s}) = x^s + \alpha_1(y_i)x^{s-1} + \alpha_2(y_i)x^{s-2} + \ldots + \alpha_s(y_i)$$

Abbiamo dunque

$$f(x) = \prod_{i=1}^{i=2}\left[x^s + \alpha_1(y_i)x^{s-1} + \alpha_2(y_i)x^{s-2} + \ldots\ldots + \alpha_s(y_i)\right]$$

il che significa che: l'equazione $f(x)=0$ è il risultato che si ottiene eliminando y fra le due equazioni

$$\begin{cases} \Phi(y) = y^r + c_1 y^{r-1} + c_2 y^{r-2} + \ldots\ldots + c_{r-1}y + c_r = 0 \\ x^s + \alpha_1(y)x^{s-1} + \alpha_2(y)x^{s-2} + \ldots\ldots + \alpha_s(y) = 0 \end{cases}$$

Viceversa se la proposta è un risultato di eliminazione fra due equazioni della forma precedente il suo gruppo, come facilmente si vede, è imprimitivo.

§ 69. — **Riduzione di un'equazione composta a successive equazioni semplici.** — Arriviamo alla parte più importante della teoria di Galois, a ricercare cioè come la **composizione** del gruppo di Galois per un'equazione $f(x)=0$ si rifletta in corrispondenti proprietà della equazione. — Per esprimerci più brevemente chiameremo (in un dato campo di razionalità) **composta** una equazione quando il suo gruppo di Galois è composto, **semplice** invece quando il gruppo stesso è semplice. — Ed ora dimostriamo: **Alla risoluzione di un'equazione composta** $f(x)=0$ **può sostituirsi la risoluzione successiva**

di equazioni ausiliarie (risolventi) semplici.-
Sia G il gruppo di Galois per la $f(x)=0$; e supponendo lo composto indichiamo con G_1 un suo sottogruppo invariante massimo.- Prendiamo secondo il §66, una funzione razionale $y_1 = \psi(x_1\, x_2 \ldots x_n)$
delle radici della proposta il cui gruppo numerico sia precisamente G_1 e con essa costruiamo la corrispondente risolvente $\Phi_{e_1}(y)=0$
il cui grado e_1 eguaglierà l'indice di G_1 in G.-
Il gruppo di questa risolvente sarà precisamente pel §67 il gruppo fattoriale $H=\frac{G}{G_1}$ che è un gruppo semplice essendo G_1 invariante massimo in G (§ 23).-
Il gruppo H transitivo sulle e_1 radici
$$y_1\ y_2 \ldots\ldots y_{e_1}$$
ha un ordine precisamente $= e_1$, cioè H è semplicemente transitivo. Ne segue che: **Qualsiasi radice della risolvente può esprimersi razionalmente per una radice fissa arbitraria, perchè in H la sola identità lascia ferma una radice arbitraria (*).-**

(*) In altre parole, come già si è osservato al § precedente, il gruppo numerico di una qualunque delle y è sempre G_1.-

Se supponiamo risolta la risolvente $\Phi_{e_1}(y)=0$, per il che basta conoscere od aggiungere al campo di razionalità una sua radice, il gruppo della proposta scende da G al sottogruppo invariante massimo G_1.

Partendo ora dal nuovo campo di razionalità da cui il gruppo di $f(x)=0$ è G_1 prendiamo un sottogruppo invariante massimo G_2 di G_1 ed indicando con e_2 il corrispondente fattore di composizione costruiamo nello stesso modo una nuova risolvente

$$\Phi_{e_2}(z)=0$$

che avrà per gruppo di Galois il gruppo $\frac{G_1}{G_2}$ e godrà delle proprietà stesse descritte per la prima risolvente, in particolare sarà una equazione semplice. La risoluzione di

$$\Phi_{e_2}(z)=0$$

cioè la conoscenza di una sua radice abbassa il gruppo della proposta da G_1 a G_2. — Così continuando è chiaro che arriviamo al seguente teorema:

Se l'equazione proposta $f(x)=0$ ha per gruppo di Galois un gruppo composto G di cui sia

$$G, G_1, G_2 \ldots\ldots G_\nu, 1$$

una serie di composizione coi fattori di composizione $e_1, e_2, \ldots\ldots e_\nu$, la sua risoluzione si riduce a quella di successive risolventi semplici $\Phi_{e_1}(y)=0$,

$\Phi_{e_1}(z)=0$, ... $\Phi_{e_2}(t)=0$ i cui gradi coincidono coi rispettivi fattori di composizione di G e i corrispondenti gruppi di Galois coi gruppi fattoriali di G.– Tutte queste equazioni ausiliarie sono semplici ed ogni loro radice è razionalmente esprimibile per una qualunque di esse.–
Così la nostra asserzione è dimostrata e il teorema di Jordan sull' invariabilità dei fattori di composizione, come quello di Hölder sull' invariabilità dei gruppi fattoriali appariscono ora sotto nuova luce.– Essi ci dimostrano che in questa riduzione di un' equazione composta a successive equazioni ausiliarie semplici possiamo benissimo eseguire in diversi modi queste equazioni ausiliarie, però i loro ordini e i loro gruppi di Galois restano sempre gli stessi.

§70.– **Equazioni Abeliane.**– Andiamo ora ad applicare i teoremi fondamentali fin qui esposti ad una importante classe di equazioni che dicesi **Abeliane**, perchè Abel fu il primo a considerarle in tutta la loro generalità. Diciamo **Abeliana** ogni equazione il cui gruppo di Galois sia un gruppo Abeliano (§ 31) cioè un gruppo le cui sostituzioni siano due a due permutabili.–

Se l'equazione Abeliana $f(x)=0$ è riducibile, essa si spezza nel prodotto di più equazioni Abeliane irriducibili. - E invero se le n radici si dividono in più sistemi di transitività

$$(x_1 x_2 \ldots x_i),\ (x_{i+1} \ldots x_k) \ldots\ldots$$

il gruppo Abeliano G della equazione sarà il prodotto di più gruppi parziali Abeliani transitivi

$$T, T', T'' \ldots\ldots$$

nei singoli sistemi ed i corrispondenti fattori irriducibili di $f(x)$

$$f_1(x) = (x-x_1)\ldots(x-x_i)$$

$$f_2(x) = (x-x_{i+1})\ldots(x-x_k)$$

uguagliati a zero daranno altrettante equazioni Abeliane coi rispettivi gruppi $T, T' \ldots$.

Ora supposta l'equazione Abeliana di grado n

$$f(x)=0$$

irriducibile, è facile vedere in primo luogo che il suo gruppo G è precisamente d'ordine n. Ed infatti se una sostituzione S di G lascia ferma una radice p. es. x_1 vi sarà nel gruppo transitivo G una sostituzione σ che trasporta x_1 in x_i e la $\sigma^{-1} S \sigma = S$ lascierà ferma anche x_i, onde segue che S è l'identità. - Dunque l'ordine di G è precisamente $= n$ e noi indicheremo con g_i quella sua sostituzione perfetta

mente determinata che porta x_1 in x_i. – Se aggiungiamo al campo di razionalità una radice p. es. x_1, anche tutte le altre riusciranno note, abbassandosi G all' identità; avremo dunque

$$x_i = \theta_i(x_1) \qquad x_k = \theta_k(x_1)$$

indicando θ_i, θ_k funzioni razionali intere, di grado $n-1$ al più, del loro argomento. – Se alla loro differenza $x_i - \theta_i(x_i) = 0$, razionalmente nota, applichiamo la g_k ed indichiamo con x_l la radice in cui è portata la x_1 dal prodotto $g_i g_k$ ne deduciamo

$$x_l = \theta_i\left[\theta_k(x_1)\right] ;$$

ma poichè $g_i g_k = g_k g_i$, ne deduciamo altresì

$$x_l = \theta_k\left[\theta_i(x_1)\right] ,$$

dunque: **Ogni equazione Abeliana irriducibile gode della proprietà che per una sua radice qualunque, p. es. x_1, sono esprimibili razionalmente tutte le altre e se $\theta_i(x_1)$, $\theta_k(x_1)$ sono due radici qualsiasi si ha $\theta_i\left(\theta_k(x_1)\right) = \theta_k\,\theta_i(x_1)$, cioè le operazioni θ eseguite sulle radici sono due a due invertibili.** –

È facile dimostrare inversamente che se un' equazione irriducibile gode della proprietà enunciata, rispetto ad una particolare radice per la quale si suppone che tutte

le altre si esprimano razionalmente, l'equazione sarà abeliana e la proprietà stessa varrà quindi per ogni altra radice.- Supponiamo infatti che per la radice x_1 possano esprimersi razionalmente tutte le altre ed abbia in oltre luogo la detta invertibilità delle operazioni θ corrispondenti. Aggiungendo al campo di razionalità x_1, il gruppo G si abbassa all'identità quindi non vi è in G alcuna sostituzione, eccetto l'identità, che lasci ferma x_1 e però G è semplicemente transitivo.-

Siano g, g' due sostituzioni qualunque del gruppo (transitivo) di Galois che portino rispettivamente x_1 in x_i, x_k e sia

$$x_i - \theta_i(x_1) = 0 \qquad x_k - \theta_k(x_1) = 0$$

Se indichiamo con x_2 la radice in cui il prodotto gg' porta x_1, con x_3 la radice in cui il prodotto $g'g$ porta x_1 stessa, applicando alla prima relazione la g', alla seconda la g dedurremo $x_2 = \theta_i[\theta_k(x_1)]$, $x_3 = \theta_k[\theta_i(x_1)]$

quindi $x_2 = x_3$.- Dunque i prodotti gg', $g'g$ portano x_1 al medesimo e quindi coincidono perchè, come sopra si è osservato, la sola identità lascia ferma x_1.- Così avendosi per due sostituzioni qualsiasi di G

$$gg' = g'g$$

il gruppo è Abeliano c. d. d.-

§ 71. – **Risoluzione per radicali di un'equazione Abeliana a gruppo ciclico.** – Se applichiamo il risultato generale ottenuto nel § 69 ad un'equazione Abeliana composta, vediamo subito che le successive equazioni ausiliarie semplici (risolventi) saranno anch'esse Abeliane e inoltre i loro gradi eguagliando i fattori di composizione del gruppo Abeliano saranno altrettanti numeri primi (§ 32). – Precisamente se si decompone il grado n dell'equazione Abeliana data nei suoi fattori primi diversi

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r},$$

dovremo successivamente risolvere α_1 equazioni Abeliane di grado p_1, α_2 di grado p_2 ecc ecc. –

Basterebbe dunque occuparsi della risoluzione di un'equazione Abeliana irriducibile di grado primo p. – Il gruppo di una tale equazione consta evidentemente delle p potenze di una sostituzione ciclica sulle p radici e noi generalizziamo la ricerca considerando una equazione Abeliana di grado qualsiasi n.

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots\ldots + a_{n-1} x + a_n$$

Il cui gruppo consti delle potenze di una sostituzione ciclica

$$S = (x_0\ x_1 \ldots\ldots x_{n-1})$$

sulle

n radici.- Qui indichiamo per comodità le n radici coi gli indici $0, 1, 2, \ldots n-1$ presi (mod n) e riguardiamo $x_r = x_s$ quando $r \equiv s \pmod n$.-

Per una tale equazione avremo

$$x_1 = \theta(x_0)$$

essendo θ una funzione razionale intera di x_1 (di grado minore di n).- Applicando alla relazione precedente la sostituzione S e le sue potenze e ponendo per brevità

$$\theta[\theta(x_0)] = \theta^2(x_0) \;,\; \theta(\theta^2(x_0)) = \theta^3(x_0) \ldots\ldots\ldots$$

troviamo $x_1 = \theta(x_0)$, $x_2 = \theta^2(x_0) \ldots\ldots x_{n-1} = \theta^{n-1}(x_0)$, $x_0 = \theta^n(x_0)$

Le radici della equazione Abeliana formano in tal caso, come si dice, un unico periodo.- Viceversa se le radici di una equazione Abeliana irriducibile formano un unico periodo $x_0 \;,\; \theta(x_0) \;,\; \theta^2(x_0) \ldots\ldots \theta^{n-1}(x_0)$

si vede subito che il suo gruppo sarà il gruppo ciclico generato dalle potenze della sostituzione

$$S = \left(x_0 \;,\; \theta(x_0) \;,\; \theta^2(x_0) \ldots\ldots \theta^{n-1}(x_0)\right).-$$

Indicando con ε una radice n^{ma} qualsiasi della unità consideriamo la funzione razionale delle radici della proposta

$$x_0 + \varepsilon x_1 + \varepsilon^2 x_2 + \ldots\ldots + \varepsilon^{n-1} x_{n-1}$$

(i cui coefficienti contengono la quantità aggiunta ε) e adottiamo la notazione $(\varepsilon, x_0) = x_0 + \varepsilon x_1 + \varepsilon^2 x_2 + \ldots\ldots + \varepsilon^{n-1} x_{n-1}$

Se a questa funzione y_1 delle radici applichiamo la sostituzione fondamentale $S = (x_0\, x_1 \ldots x_{n-1})$ del gruppo di Galois ne otteniamo

$$y_S = x_1 + \varepsilon x_2 + \varepsilon x_3 + \cdots\cdots + \varepsilon^{n-1} x_0 = \varepsilon^{-1} y_1 ,$$

onde segue che la sua n^{ma} potenza

$$y_1^n = (\varepsilon, x_0)^n$$

rimane numericamente invariata effettuandovi la S e le sue potenze e però essa è razionalmente esprimibile per le quantità primitive del campo e per ε.—
Ora se diamo ad r il significato di una radice primitiva n^{ma} dell'unità, le quantità

$$(\varepsilon^r, x_0)^n = B_r$$

saranno razionalmente note e però le (ε^r, x) si otterranno estraendo una radice n^{ma}. — Dalle n equazioni lineari

$$\begin{cases} (1, x_0) = x_0 + x_1 + \cdots\cdots + x_{n-1} = -a_1 \\ (\varepsilon, x_0) = x_0 + \varepsilon x_1 + \cdots\cdots + \varepsilon^{n-1} x_{n-1} = \sqrt[n]{B_1} \\ (\varepsilon^2, x_0) = x_0 + \varepsilon^2 x_1 + \cdots\cdots + \varepsilon^{2(n-1)} x_{n-1} = \sqrt[n]{B_2} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ (\varepsilon^{n-1}, x_0) = x_0 + \varepsilon^{n-1} x_1 + \cdots\cdots + \varepsilon^{(n-1)^2} x_{n-1} = \sqrt[n]{B_{n-1}} \end{cases}$$

sommando coll'osservare che si ha per $r \not\equiv 0 \pmod n$

$$1 + \varepsilon^r + \varepsilon^{2r} + \cdots\cdots + \varepsilon^{(n-1)r} = \frac{\varepsilon^{nr} - 1}{\varepsilon^r - 1} = 0$$

resulta

$$(A) \qquad x_0 = \frac{-a_1 + \sqrt[n]{B_1} + \sqrt[n]{B_2} + \cdots\cdots + \sqrt[n]{B_{n-1}}}{n} ,$$

formola che ci fa conoscere con estrazioni di radicali la prima radice x_0.– Le altre possono dedursi razionalmente da x_0 ovvero direttamente dalle equazioni lineari stesse con che si ottiene

$$x_2 = \frac{-a_1 + \varepsilon^{-2}\sqrt[n]{B_1} + \varepsilon^{-2\cdot 2}\sqrt[n]{B_2} + \ldots + \varepsilon^{-(n-1)2}\sqrt[n]{B_{n-1}}}{n}$$

ciascuno degli $n-1$ radicali che compariscono in questa formola di risoluzione (A) è suscettibile di n diverse determinazioni; ma, come ora dimostreremo, basta dare al primo radicale i suoi n valori, gli altri radicali potendo esprimersi razionalmente per questo.–

§72.– **Modificazione della formola (A) di risoluzione.**– Per compiere la modificazione enunciata per la formola (A) conviene risalire al significato che ha per noi $\sqrt[n]{B_2}$ e cioè

$$\sqrt[n]{B_2} = (\varepsilon^2, x_0)$$

Applicando la sostituzione fondamentale S del gruppo di Galois, per quanto sopra abbiamo osservato, la funzione (ε, x_0) si moltiplica per ε^{-1} e similmente la (ε^2, x_0) per ε^{-2} onde il prodotto

$$(\varepsilon^2, x_0)(\varepsilon, x_0)^{n-2} = \sqrt[n]{B_2} \cdot (\sqrt[n]{B_1})^{n-2}$$

è razionalmente noto; poniamo dunque $\sqrt[n]{B_2}(\sqrt[n]{B_1})^{n-2} = C_2$,

essendo c_2 una quantità razionalmente nota (nel campo ampliato con l'aggiunta di ε). Se supponiamo dunque che sia $\sqrt[n]{B_1} = (\varepsilon, x_0) \neq 0$ avremo

$$\sqrt[n]{B_2} = \frac{c_2}{B_1}\left(\sqrt[n]{B_1}\right)^2$$

e la formola (H) di risoluzione prenderà la nuova forma

$$(B) \qquad x_0 = \frac{1}{n}\left\{-a_1 + \sqrt[n]{B_1} + \frac{c_2}{B_1}\left(\sqrt[n]{B_1}\right)^2 + \frac{c_3}{B_1}\left(\sqrt[n]{B_1}\right)^3 + \cdots + \frac{c_{n-1}}{B_1}\left(\sqrt[n]{B_1}\right)^{n-1}\right\}$$

nella quale dando a $\sqrt[n]{B_1}$ i suoi n valori si otterranno, come subito si vede, tutte le n radici.–

La trasformazione della formola (A) nella (B) suppone, come si è avvertito, che non sia

$$(\varepsilon,\ x_0) = 0.–$$

Se questo caso eccezionale si presenta potremo eliminare la difficoltà colle osservazioni seguenti (*).–

Essendo ε una radice primitiva n^{ma} della unità e p un fattore primo di n possiamo sempre trovare un conveniente esponente $\lambda \not\equiv 0 \pmod p$ tale che sia

$$(\varepsilon^\lambda, x_0) \neq 0$$

Abbiamo infatti

$$n\,x_0 = \sum_{\lambda=0}^{\lambda=n-1} (\varepsilon^\lambda, x_0)$$

$$n\,x_2 = \sum_{\lambda=0}^{\lambda=n-1} \varepsilon^{-\lambda 2} (\varepsilon^\lambda, x_0)$$

(*) Weber T. I pag. 547.–

e però $n(x_1 - x_0) = \sum_{\lambda=0}^{\lambda=n-1} (\varepsilon^{-\lambda_2} - 1)(\varepsilon^{\lambda}, x_0)$

Se poniamo $n = pq$ avremo dunque

$$n(x_q - x_0) = \sum_{\lambda} (\varepsilon^{-\lambda_q} - 1)(\varepsilon^{\lambda}, x_0)$$

Il primo fattore sotto il segno Σ, $\varepsilon^{-\lambda_q} - 1$ si annulla tutte le volte che λ è divisibile per p, quindi se il secondo si annullasse sempre quando $\lambda \not\equiv 0 \pmod p$ ne verrebbe $x_q = x_0$ cioè la proposta avrebbe radici eguali.-

Ciò premesso, scindiamo n nei suoi fattori primi diversi e sia

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_z^{\alpha_z};$$

poniamo inoltre per brevità

$$n_1 = \frac{n}{p_1^{\alpha_1}}, \quad n_2 = \frac{n}{p_2^{\alpha_2}} \ldots\ldots n_z = \frac{n}{p_z^{\alpha_z}}$$

e scegliamo, come è possibile per quanto precede,

$$\lambda_1 \not\equiv 0 (\mathrm{mod}\, p_1), \quad \lambda_2 \not\equiv 0 (\mathrm{mod}\, p_2) \ldots\ldots \quad \lambda_z \not\equiv 0 (\mathrm{mod}\, p_z)$$

in guisa che si abbia

$$(\varepsilon^{\lambda_1}, x_0) \not\equiv 0, \quad (\varepsilon^{\lambda_2}, x_0) \not\equiv 0 \ldots\ldots (\varepsilon^{\lambda_z}, x_0) \not\equiv 0$$

La quantità $(\varepsilon^{\lambda_1}, x_0)^{n_1 p_1^{\alpha_1}}$ è razionalmente nota $= \gamma_1$ onde

$$(\varepsilon^{\lambda_1}, x_0)^{n_1} = \sqrt[p_1^{\alpha_1}]{\gamma_1}, \quad (\varepsilon^{\lambda_2}, x_0)^{n_2} = \sqrt[p_2^{\alpha_2}]{\gamma_2} \ldots\ldots$$

$$\ldots\ldots (\varepsilon^{\lambda_z}, x_0)^{n_z} = \sqrt[p_z^{\alpha_z}]{\gamma_z},$$

essendo $\gamma_1, \gamma_2, \ldots\ldots \gamma_z$ razionalmente note.- Ora potremo esprimere una qualunque delle quantità (ε^s, x_0) per le precedenti osservando che $z_1 = (\varepsilon^s, x_0)(\varepsilon^{\lambda_1}, x_0)^{m_1 \nu} (\varepsilon^{\lambda_2}, x_0)^{m_2 \nu} \ldots\ldots (\varepsilon^{\lambda_z}, x_0)^{m_z \nu}$

è razionalmente nota quando sia

$$(\lambda_1 n_1 + \lambda_2 n_2 + \cdots + \lambda_2 n_2)\nu \equiv -\delta \pmod{n},$$

perchè allora z_1 non muta di valore numerico per la S.— Ma poichè il numero $\lambda_1 n_1 + \cdots + \lambda_2 n_2$ è primo con n, esiste certo un numero ν che soddisfa alla congruenza superiore e però

$$\sqrt[n]{B_3} = (\varepsilon^3, x_0) = \frac{z_1}{\left(\sqrt[\delta_1]{\gamma_1}\ \sqrt[\delta_2]{\gamma_2} \cdots \sqrt[\delta_2]{\gamma_2}\right)^{\nu}}$$

Sostituendo questi valori di $\sqrt[n]{B_3}$ nella formola di risoluzione (A) e dando ai radicali

$$\sqrt[\delta_1]{\gamma_1},\quad \sqrt[\delta_2]{\gamma_2} \cdots \cdots \sqrt[\delta_2]{\gamma_2}$$

i loro diversi valori si avranno nuovamente tutte le radici. Possiamo ora enunciare il resultato finale col teorema:

Un equazione Abeliana a gruppo ciclico sulle n radici si risolve aggiungendo al campo di razionalità una radice primitiva n^{ma} dell'unità ed estraendo un radicale d'indice n.—

Manifestamente poi, per le osservazioni al §71, abbiamo il teorema generale: **Ogni equazione Abeliana è risolubile per radicali.—**

§73.— Caso delle equazioni Abeliane a coef=

ficienti reali.. Supponiamo ora che l'equazione Abeliana a gruppo ciclico abbia i coefficienti reali ed il campo di razionalità sia pure reale, cioè la funzione stessa $\theta(x_0)$ sia a coefficienti reali.. Allora si può dare alla formola (B) di risoluzione, come Abel stesso ha dimostrato, una forma particolare molto notevole..

Osserviamo per ciò che se l'equazione Abeliana ha una radice reale (come accade certamente se il grado n della equazione è dispari) tutte le altre radici essendo funzioni reali di questa saranno egualmente reali..

Le due quantità

$$\sqrt[n]{B_1} = (\varepsilon, x_0) = x_0 + \varepsilon x_1 + \varepsilon^2 x_2 + \cdots + \varepsilon^{n-1} x_{n-1}$$

$$\sqrt[n]{B_{n-1}} = (\varepsilon^{-1}, x_0) = x_0 + \varepsilon^{-1} x_1 + \varepsilon^{-2} x_2 + \cdots + \varepsilon^{-(n-1)} x_{n-1}$$

sono quindi in tal caso coniugate.. Ma se una radice della equazione è immaginaria e però tutte le radici sono immaginarie, allora sarà l'una di queste quantità coniugata dell'altra cangiata di segno.. È invero se supponiamo che sia x_k coniugata di x_0 da

$$x_r = \theta^r(x_0)$$

segue $$x_{r+k} = \theta^r(x_k)$$

e però x_r ha per coniugata x_{r+k} onde segue $x_{2k} = x_0$ cioè $k = \frac{n}{2}$. Ora si ha $(\varepsilon, x_0) = \sum_z \varepsilon^z x_z$, percorren-

do r un sistema completo di resti (mod r) e la coniugata di (ε, x_0) è dunque $\sum_r \varepsilon^{-r} x_{r+\frac{n}{2}}$.–

Ponendo $r+\frac{n}{2} = \rho$ ed osservando che ρ percorre con r un sistema completo di resti (mod n), la quantità precedente può scriversi

$$\sum_\rho \varepsilon^{-\rho+\frac{n}{2}} x_\rho = -\sum_\rho \varepsilon^{-\rho} x_\rho = -(\varepsilon^{-1}, x_0)$$

a causa di $\varepsilon^{\frac{n}{2}} = -1$, ciò che dimostra l'asserzione.–

La quantità

$$\sqrt[n]{B_1}\,\sqrt[n]{B_{n-1}} = c_{n-1}$$

che è razionalmente nota (§ 72.) è dunque reale e precisamente positiva o negativa secondo che l'equazione ha le radici reali o immaginarie.– Se poniamo la quantità razionalmente nota B_1 sotto la forma

$$B_1 = \rho(\cos\omega + i \operatorname{sen}\omega)$$

si avrà, per quanto abbiamo detto

$$B_{n-1} = \rho(\cos\omega - i \operatorname{sen}\omega),$$

indi

$$B_1 B_{n-1} = \rho^2 = c^n,$$

essendo c il valore assoluto di c_{n-1}.– Ne deduciamo

$$\sqrt[n]{\rho} = \sqrt{c}$$

e però $\sqrt[n]{B_1} = \sqrt{c}\left(\cos\frac{\omega+2r\pi}{n} + i \operatorname{sen}\frac{\omega+2r\pi}{n}\right)$.–

La c stessa, come le altre c_i che figurano nella formu

la di risoluzione (B) sono razionalmente note per

$$\varepsilon = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n}$$

onde alla (B) si potrà dare la forma

$$x_0 = \frac{1}{n}\Big\{ + \sqrt{c}\left(\cos\frac{\omega+2\tau\pi}{n} + i\,\mathrm{sen}\,\frac{\omega+2\tau\pi}{n}\right) + (\alpha+i\beta)\left(\cos\frac{2(\omega+2\tau\pi)}{n} + i\,\mathrm{sen}\,\frac{2(\omega+2\tau\pi)}{n}\right) + (\alpha_1+i\beta_1)\sqrt{c}\left(\cos\frac{3(\omega+2\tau\pi)}{n} + i\,\mathrm{sen}\,\frac{3(\omega+2\tau\pi)}{n}\right) + \dots\dots \Big\}$$

essendo $c, \alpha, \beta, \alpha', \beta' \dots\dots$ funzioni razionali di $\cos\frac{2\pi}{n}$, $\mathrm{sen}\,\frac{2\pi}{n}$. — Si ha quindi il teorema:

Per risolvere in un campo di razionalità reale un'equazione Abeliana ciclica di grado n basta: 1° saper dividere la circonferenza in n parti eguali; 2° saper dividere un angolo ω che si può costruire in n parti eguali; 3° estrarre la radice quadrata da una unica quantità c. —

Per stabilire questo teorema abbiamo veramente supposto che non si presenti il caso eccezionale $(\varepsilon, x_0) = 0$; ma si vede facilmente, facendo uso delle considerazioni esposte alla fine del § precedente, che il teorema è vero anche in questo caso. —

Ossia se il numero n è una potenza esatta del 2

si osserverà che tutte le costruzioni geometriche descritte sono eseguibili colla riga e col compasso.—

§ 74.— Equazioni alle radici primitive p^{me} della unità.— Fra le equazioni Abeliane a gruppo ciclico si hanno le equazioni, che Gauss per primo studiò, le equazioni cioè per la divisione del circolo in un numero qualunque di parti eguali, per le quali Gauss appunto dimostrò la risolubilità per radicali.— Tratteremo in seguito più diffusamente la teoria di Gauss, ma già dapprima ci limitiamo a ciò che è necessario di conoscere per stabilire le condizioni di risolubilità di una equazione data per radicali.—

Se p è un numero primo, l'equazione

$$(1) \qquad f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

ha per radici le $p-1$ radici primitive p^{me} della unità

$$e^{\frac{2z\pi i}{p}} \qquad z = 1, 2, 3, \ldots p-1$$

e la risoluzione di questa equazione equivale appunto alla iscrizione nel circolo del poligono regolare di p lati.— Anzi tutto dimostriamo: L'equazione (1) delle radici primitive p^{me} della unità è irriducibile.— Posto infatti $x = z + 1$ l'equazione diventa

$$\frac{(z+1)^p - 1}{z} = 0$$

cioè

$$z^{p-1} + pz^{p-2} + \frac{p(p-1)}{2} z^{p-3} + \cdots\cdots + p = 0 ,$$

il che per un teorema dimostrato al §58, prova appunto che l'equazione è irriducibile. (*). - Se poniamo

$$\varepsilon = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i \operatorname{sen}\frac{2\pi}{n}$$

tutte le altre radici si esprimeranno razionalmente per ε; inoltre possiamo ordinarle in modo che esse formino un unico periodo. - È invero indicando con g una radice primitiva del numero primo p le $p-1$ radici

$$\varepsilon, \ \varepsilon^g, \ \varepsilon^{g^2}, \ \ldots\ldots\ldots \ \varepsilon^{g^{p-2}}$$

sono distinte fra loro, perchè si ha $\varepsilon^z = \varepsilon^s$ solo quando $z \equiv s \pmod p$, ed inoltre ciascuna è la potenza g^{ma} di quella che la precede, mentre

$$\left(\varepsilon^{g^{p-2}}\right)^g = \varepsilon^{g^{p-1}} = \varepsilon .$$

Per l'osservazione al §71 vediamo dunque che il gruppo della (1) è il gruppo ciclico generato dalle potenze della sostituzione $S = (\varepsilon, \ \varepsilon^g, \ \varepsilon^{g^2}, \ \ldots\ldots \ \varepsilon^{g^{p-2}})$ -

La nostra equazione Abeliana (1) è composta e se ne scindiamo il grado $p-1$ nei suoi fattori primi, sia

---

(*) Questa è la dimostrazione di Eisenstein -

$$p-1 = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_2^{\alpha_2},$$

applicando le osservazioni generali al principio del § 71 stabiliamo il teorema seguente: Per trovare la radice primitiva p^{ma} dell'unità $\varepsilon = \cos\frac{2\pi}{p} + i \operatorname{sen}\frac{2\pi}{p}$, essendo p un numero primo e $p-1 = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_2^{\alpha_2}$, basta conoscere le radici primitive dell'unità

$$\varepsilon_1, \varepsilon_2, \ldots\ldots \varepsilon_2$$

dei rispettivi ordini

$$p_1, p_2, \ldots\ldots p_2$$

indi estrarre α radici quadrate, α_1 radicali di indice p_1, α_2 d'indice p_2 ecc.

§ 75.— Riduzione del gruppo di un'equazione per l'aggiunta delle radici di un'equazione ausiliaria.— Ritorniamo ora alle ricerche generali dei § § 66, ... allo scopo di stabilire le condizioni di risolubilità per radicali di una equazione.— La riduzione di una equazione composta a successive equazioni semplici è stata conseguita nel § 69 adoperando delle equazioni ausiliarie speciali e cioè delle risolventi della proposta.— Ora ricerchiamo se può abbassarsi il gruppo della proposta ampliando il campo di razionalità ...

aggiunta delle radici di una equazione ausiliaria qualsiasi. Stabiliremo il seguente teorema fondamentale:(*)

Se il gruppo G di Galois per una equazione

$$f(x) = 0$$

si riduce ad un suo sottogruppo G_1 per l'aggiunta di tutte le radici di un' equazione ausiliaria

$$\varphi(y) = 0 ,$$

viceversa il gruppo T di questa si ridurrà ad un suo sottogruppo T_1 per l'aggiunta di tutte le radici della primitiva, inoltre G_1 sarà invariante in G, T_1 in T e i gruppi complementari $\frac{G}{G_1}$, $\frac{T}{T_1}$ saranno identici. (oloedricamente isomorfi)

Siano n, m i rispettivi gradi di $f(x)=0$, $\varphi(y)=0$ e

$$x_1 \; x_2 \ldots\ldots x_n$$

$$y_1 \; y_2 \ldots\ldots y_m$$

le loro radici. Indichiamo poi con $\underline{r}$ il grado di G, con r_1 quello del sottogruppo G_1 e con s quello di T. Costru-

---

(*) Il teorema è dovuto a Jordan (Traité des substitutions pag 269-70) e completato da Holder nel modo qui esposto (Maths. Annalen 34)

riamo una funzione razionale delle radici della proposta $z_1 = \varphi_1(x_1\ x_2 \ldots\ x_n)$ il cui sottogruppo numerico sia precisamente G_1 (§ 66) e con essa costruiamo una risolvente della proposta

$$\Theta(z) = 0$$

che avrà per grado $\frac{\tau}{\tau_1}$ e per gruppo il gruppo complementare $\frac{G}{G_1}$ (§ 67). — Se al campo attuale di razionalità si aggiungono le radici $y_1\ y_2 \ldots\ y_m$ dell'ausiliaria $\varphi(y) = 0$, il gruppo G della proposta scende, per ipotesi, a G_1 e però z_1 è razionalmente esprimibile per $y_1, y_2 \ldots y_m$, sia

$$z_1 = \varphi_1(x_1 x_2 \ldots x_n) = \Phi_1(y_1\ y_2 \ldots y_m) \text{ —}$$

Indichiamo ora con T_1 il sottogruppo numerico di T per la funzione $\Phi_1(y_1\ y_2 \ldots y_m)$ e formiamo con questa la risolvente di $\varphi(y) = 0$, che avrà l'ordine $\frac{\sigma}{\sigma_1}$, se σ_1 è l'ordine di T_1, e il gruppo $\frac{T}{T_1}$. — Ma questa risolvente, che è irriducibile come la $\theta(z) = 0$, ha con essa a comune la radice $\varphi_1(x_1\ x_2 \ldots x_n) = \Phi_1(y_1\ y_2 \ldots y_m)$; dunque le due risolventi coincidono e si ha quindi intanto

$$\frac{\tau}{\tau_1} = \frac{\sigma}{\sigma_1} \quad , \quad \frac{G}{G_1} = \frac{T}{T_1}.$$

Se indichiamo con $z_1, z_2 \ldots z_q$ le $q = \frac{\tau}{\tau_1}$ radici della risolvente $\theta(z) = 0$, aggiunte al campo di ra-

zionalità $y_1\ y_2 \ldots y_m$ è nota non soltanto la prima radice z_1 di $\theta(z)$, ma anche tutte le altre perchè razionali in $y_1, y_2 \ldots y_m$. — Dunque, considerate come funzioni delle x, le $z_1, z_2 \ldots z_m$ hanno tutte il medesimo sottogruppo numerico G_1 che è adunque invariante in G; ne segue che $z_2, z_3, \ldots z_m$ sono funzioni razionali di z_1. — Ora aggiungiamo al campo di razionalità le radici $x_1\ x_2 \ldots x_n$ della primitiva ed osserviamo che cosa diventerà il gruppo di Galois della ausiliaria $\varphi(y) = 0$. Siccome $z_1 = \Phi_1(y_1 y_2 \ldots y_m) = \varphi_1(x_1 x_2 \ldots x_n)$ dopo tale aggiunta viene ad essere razionalmente nota, il gruppo T si abbasserà o a T_1 o ad un sottogruppo di T_1. — Ma l'ultima ipotesi si esclude facilmente poichè intanto vediamo che l'indice in T del sottogruppo T_2 cui si abbassa T per l'aggiunta delle radici della $f(x) = 0$ sarà

$$q' \geq q$$

essendo q l'indice del sottogruppo G_1 del gruppo G di $f(x) = 0$ a cui si abbassa G per l'aggiunta delle y. — Ma allora, scambiando in questo risultato le due equazioni $f(x) = 0$, $\varphi(y) = 0$, vediamo che si deve avere altresì

$$q \geq q'$$

indi $q' = q$ e $T_2 = T_1$, ciò che dimostra completamente il

teorema.—

Come corollario del nostro teorema notiamo che se l'equazione ausiliaria è semplice, avendosi $T_1 = 1$, ogni sua radice sarà nota quando al campo di razionalità si aggiungono $x_1\ x_2 \ldots x_n$, cioè Ogni equazione ausiliaria semplice la cui risoluzione contribuisca all'abbassamento del gruppo della proposta è necessariamente una risolvente di questa.—

D'altra parte potendosi sostituire ad ogni equazione ausiliaria composta, col teorema del §69, una successione di equazioni ausiliarie semplici, che sono dunque risolventi della proposta, vediamo che la generalizzazione introdotta col considerare equazioni ausiliarie qualunque invece di risolventi è soltanto apparente ed il teorema citato del §69 ci dà tutto ciò che si può conseguire per la risoluzione della proposta con successive equazioni ausiliarie.—

Notiamo infine che se la proposta è un'equazione semplice, qualunque equazione ausiliaria semplice, la cui risoluzione abbassi il gruppo della proposta, lo riduce all'identità; ma allora l'ausiliaria ha il medesimo gruppo della primitiva.—

§76.— Condizioni di risolubilità per radicali.— Siamo ora in grado di trovare le condizioni di risolubilità per radicali di un' equazione $f(x)=0$. Supponiamo per ciò dapprima che i fattori di composizione

$$p_1, p_2, \ldots\ldots p_z$$

del suo gruppo siano numeri primi. Se applichiamo il teorema generale del §69, vediamo che le successive equazioni ausiliarie semplici

$$\Phi_{p_1}(y)=0 \quad , \quad \Phi_{p_2}(z)=0 \ldots\ldots$$

sono equazioni Abeliane di grado primo a gruppo ciclico e però risolubili con ispettive estrazioni di radicali d' indici $p_1, p_2, \ldots\ldots p_z$ e coll' aggiunta delle corrispondenti radici dell' unità

$$\varepsilon_1, \varepsilon_2 \ldots\ldots \varepsilon_z$$

d' ordini $p_1, p_2, \ldots\ldots p_z$.— Dunque: Se il gruppo G di un' equazione ha per fattori di composizione altrettanti numeri primi

$$p_1, p_2 \ldots\ldots p_z$$

l' equazione si risolve estraendo successivi radicali d' indici eguali a questi fattori primi.(*)

(*) Sottintendiamo che siano aggiunte le radici corrispon-

Ora ci proponiamo di dimostrare inversamente che se un'equazione $f(x)=0$ è risolubile per radicali, i fattori di composizione del suo gruppo saranno altrettanti numeri primi.- Noi supponiamo adunque che le radici di $f(x)=0$ possano esprimersi per mezzo di successive estrazioni di radici da effettuarsi sopra quantità note o che tali diventano dopo l'aggiunta di radicali precedenti. Aggiungendo via via i vari radicali che si presentano nella soluzione, da ultimo il gruppo della equazione proposta dovrà trovarsi ridotto all'identità, l'equazione essendo risoluta.- Ora estrarre un radicale di indice composto equivale ad estrarre successivi radicali di indice primo e quindi possiamo dire che il gruppo di $f(x)=0$ dovrà ridursi all'identità aggiungendo successivamente le radici di equazioni ausiliarie binomie della forma (2) $z^p = A$, dove p è un numero primo ed A una quantità nota o razionalmente esprimibile per quelle prime aggiunte.-
Indicando con z_1 una radice della (2) saranno

---

centi dell'unità $\varepsilon_1, \varepsilon_2 \ldots \varepsilon_2$, come è necessario per avere ai radicali tutti i loro valori.-

$$z_1, z_2 = \varepsilon z_1, \quad z_3 = \varepsilon^2 z_1, \dots z_{p-1} = \varepsilon^{p-1} z_1 \quad \left(\varepsilon = e^{\frac{2\pi i}{p}}\right)$$

tutte le sue radici, sicchè, ampliato il campo di razionalità col l'aggiunta di ε, la (2) è un'equazione Abeliana. Se la supponiamo riducibile, per quanto abbiamo rilevato al § 60, dovrà spezzarsi in fattori di egual grado r e dovendo essere r un divisore primo di p sarà $r=1$ cioè tutte le radici di (2) saranno allora razionali in ε(*) e l'aggiunta del radicale $\sqrt[p]{A}$ potrà senz'altro omettersi. Supposto che ciò non accada, il gruppo della (2) è dunque un gruppo ciclico Γ_p sulle p radici ed applicando il teorema fondamentale del § precedente ne deduciamo quindi:

(*) La stessa cosa può dimostrarsi direttamente così: Le $z_1, z_2 \dots z_\nu$ sono le radici di un fattore irriducibile della (2), deve dunque $\nu < p$, in particolare il loro prodotto $z_1 z_2 \dots z_\nu$ sarà una quantità K razionalmente nota, onde avremo una eguaglianza della forma

$$\varepsilon^\alpha z_1^\nu = K$$

Risolviamo in numeri interi α, β l'equazione $p\alpha + \nu\beta = 1$ dopo di che elevando la precedente uguaglianza alla potenza β col l'osservare che $z_1^p = A$, troviamo

$$z_1 = A^\alpha K^\beta \varepsilon^{-\alpha\beta}$$

il che dimostra che $z_1, z_2 \dots z_p$ sono razionali in ε. C. D. D.

a) Se aggiunta la radice p^{ma} dell'unità ε, il gruppo della proposta è $\mathfrak{G}$ e per la successiva aggiunta di un radicale d'indice p $\sqrt[p]{A}$, il gruppo $\mathfrak{G}$ si abbassa, esso si ridurrà ad un suo sottogruppo invariante $\mathfrak{G}_1$ d'indice p.

Resta ora che vediamo quale abbassamento può aver prodotto nel primitivo gruppo dell'equazione l'aggiunta della radice p^{ma} dell'unità e per ciò dimostreremo:

b) Se il gruppo $\mathfrak{G}'$ della proposta scende, per l'aggiunta della radice p^{ma} dell'unità ε ad un suo sottogruppo $\mathfrak{G}_1$ sarà $\mathfrak{G}$ invariante in $\mathfrak{G}'$ e fra $\mathfrak{G}'$ e $\mathfrak{G}$ potrà inserirsi una serie di sottogruppi

$$\mathfrak{G}' H H_1 H_2 \cdots \mathfrak{G}$$

tali che ciascuno sia invariante nel precedente ed abbia per indice un numero primo.

E invero aggiungendo ε noi aggiungiamo tutte le radici dell'equazione Abeliana.

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = 0$$

il cui gruppo attuale Γ' sarà o il gruppo ciclico dell'equazione stessa nel campo assoluto di razionalità (§ 74) o un suo sottogruppo. Dunque $\mathfrak{G}$ è certamente invariante in $\mathfrak{G}'$ ed esiste pel teorema fondamentale al § 75 in Γ' un sottogruppo invariante [illegible] i gruppi complementari

$\frac{\Sigma'}{\Sigma}$, $\frac{\Gamma'}{\Gamma}$

sono descrivicamente isomorfi. Ma essendo Γ' un gruppo Abeliano e Γ un suo sottogruppo è certo possibile per le proprietà dei gruppi Abeliani (5ª 1ª §. 52) inserire fra Γ', Γ una serie di sottogruppi i cui fattori di composizione siano numeri primi onde anche fra Σ', Σ potremo inserire i sottogruppi H richiesti.

§ 71.— Irresolubilità per radicali delle equazioni generali di grado $n > 4$ — Rimendo i resultati ottenuti nel § prec. otteniamo il teorema finale:

Affinchè un'equazione sia risolubile per radicali è necessario e sufficiente che i fattori di composizione del suo gruppo siano altrettanti numeri primi.

Per questa ragione appunto si chiamano gruppi risolubili quelli i cui fattori di composizione sono numeri primi.

Come abbiamo visto al § 65 l'equazione generale di grado n ha per gruppo il gruppo totale $\Sigma_{\Pi(n)}$. I fattori di composizione di questo gruppo se $n > 4$ sono (5ª 1ª §.)

$$2 \quad e \quad \frac{\Pi(n)}{2},$$ onde concludiamo:

Le equazioni generali di grado superiore al quarto non sono risolubili per radicali.

Ciò vale in particolare della equazione generale di 5° grado co

frei primi dimostrarono Ruffini ed Abel (*).
L'unico abbassamento possibile nel gruppo dell'equazione generale di grado n è quella che si ottiene aggiungendo al campo di razionalità la radice quadrata del discriminante

$$\Delta = \Pi (x_\alpha - x_\beta)^2.$$

Siccome $\sqrt{\Delta}$ è una funzione invariabile per le sostituzioni pari, la sua aggiunta abbassa il gruppo dell'equazione al gruppo alterno $\mathfrak{G}_{\frac{\Pi(n)}{2}}$ dopo di che sono razionalmente note non solo le funzioni simmetriche delle radici, ma ben anche le semisimmetriche cioè quelle invariabili per le sostituzioni di $\mathfrak{G}_{\frac{\Pi(n)}{2}}$, che possono esprimersi tutte sotto la forma

$$A + B\sqrt{\Delta},$$

essendo A, B razionali nei coefficienti della equazione. Ma il gruppo $\mathfrak{G}_{\frac{\Pi(n)}{2}}$ essendo semplice, qualunque ulteriore abbassamen-

---

(*) Le dimostrazioni date da Ruffini non possono considerarsi completamente rigorose come quella d'Abel. Tuttavia è negli scritti di questo geometra italiano che trovansi i primi germi della teoria dei gruppi di sostituzioni elaborata poi da Cauchy e Galois (Vedi Burckhardt - Die Anfänge der Gruppentheorie und Paolo Ruffini. - Traduzione di E. Pascal negli annali di matematica - Anno 1894).

to del gruppo per estrazioni di radicali, o per aggiunta delle radici di equazioni ausiliari, è impossibile.

Come abbiamo poi dimostrato al §. 65, non solo le equazioni generali di grado n ma persino equazioni a coefficienti numerici hanno, nel campo assoluto di razionalità, per gruppo il gruppo totale e sono quindi insolubili per radicali. Tale è per esempio (v. § 65) l'equazione di 5° grado

$$x^5 + 5x^2 - 5x - 5 = 0.$$

Se applichiamo i teoremi ottenuti alle equazioni generali di grado $n = 2, 3, 4$, vediamo chiaramente perchè esse sono risolubili per radicali. Per $n = 2$ l'aggiunta della radice quadrata del discriminante abbassa il gruppo all'identità (gruppo alterno) e l'equazione è risoluta.

Per $n = 3$ abbiamo la serie di composizione

$\mathfrak{S}_6$	$\mathfrak{S}_3$	1
gruppo totale	gruppo alterno	identità
coi fattori	2	3

L'estrazione della radice quadrata del discriminante abbassa il gruppo al gruppo ciclico $\mathfrak{S}_3$ e l'equazione, che diventa allora Abeliana, si risolve estraendo un radicale cubico.

Per $n = 4$ la serie di composizione è:

G_{24} G_{12} G_4 G_2 1

gruppo totale gruppo totale
coi fattori di composizione

2 3 2 2

L'estrazione di una prima radice quadrata, (quella del discriminante) abbassa il gruppo a G_{12} quella di un radicale cubico a G_4 e le successive estrazioni di due radici quadrate risolvono poi l'equazione.

Applicando il teorema generale del § 69 per la effettiva costruzione delle successive risolventi si ottengono appunto le ordinarie formole di risoluzione per le equazioni di 3° e 4° grado.

§ 78. — Risolubilità generale per radicali. Le ricerche precedenti sono relative alla completa risolubilità per radicali di una equazione. Si potrebbe peraltro pensare che esistessero equazioni irriducibili, di cui una o più radici si potessero esprimere per radicali senza che ciò fosse possibile per tutte. Naturalmente se si tratta di equazioni riducibili ciò è ben possibile; ma per equazioni irriducibili possiamo dimostrare il teorema:

"Una equazione irriducibile di cui una o più radi

ci possono esprimersi per radicali è totalmente risolubile per radicali.

Nelle memorie di Abel tale proprietà è enunciata dicendo che se ad una equazione irriducibile si può soddisfare algebricamente è risolubile algebricamente (per radicali).

Supponiamo adunque che per successive estrazioni di radicali si pervenga a conoscere una o più radici di una equazione irriducibile di grado n e come al §. 76 seguano via via l'abbassamento prodotto nel gruppo della equazione per queste successive aggiunte. Il gruppo che era primitivamente transitivo sarà diventato intransitivo quando le aggiunte dei successivi radicali avranno resa razionalmente nota una radice. Poniamo che il primo abbassamento da un gruppo transitivo G ad uno intransitivo G_1 abbia luogo per l'aggiunta di un radicale d'indice primo p, sia $\sqrt[p]{A}$. Pel teorema a/ §76 sarà G_1 invariante d'indice p in G e poichè G_1 è intransitivo e G transitivo, le n lettere

$$x_1\ x_2 \cdots x_n$$

su cui opera G_1 si scinderanno, rispetto a G_1 in sistemi di transitività contenenti tutti un egual numero r di lettere, come si vede ripetendo un ragionamento che ab-

biamo fatto al §. 34 P.e 1°. Dunque intanto se il grado n della nostra equazione è un numero primo, sarà $r=1$ cioè tutte le radici risulteranno note e l'equazione sarà totalmente risolubile per radicali, come è enunciato nel teorema. In generale se

$$(x_1, x_2 \cdots x_r)\ ,\ (x_{r+1}\ x_{r+2} \cdots x_{2r})\ , \cdots\cdots\cdots$$

sono i sistemi d'imprimitività, saranno

$$\varphi_1(x, \sqrt[p]{A}) = (x-x_1)(x-x_2)\cdots(x-x_r)$$
$$\varphi_2(x, \sqrt[p]{A}) = (x-x_{r+1})(x-x_{r+2})\cdots(x-x_{2r})$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

i vari fattori irriducibili di $f(x)$ nel campo ampliato coll'aggiunta di $\sqrt[p]{A}$.

Ora il gruppo intransitivo $\mathfrak{S}_1$ è il prodotto di varii gruppi parziali

$$\Gamma_1\ \Gamma_2\ \Gamma_3 \cdots$$

operanti (transitivamente) sopra le lettere dei singoli sistemi. Questi gruppi $\Gamma_1, \Gamma_2 \cdots$ sono i rispettivi gruppi di Galois per le equazioni

$$\varphi_1(x, \sqrt[p]{A}) = 0\ ,\quad \varphi_2(x, \sqrt[p]{A}) = 0\ , \cdots$$

Ora osservando che $\mathfrak{S}_1$ è invariante nel gruppo transitivo $\mathfrak{S}$ si vede subito che $\Gamma_1\ \Gamma_2\ \Gamma_3 \cdots$ sono fra loro olo-edricamente isomorfi per cui se l'equazione

$$\varphi_1(x, \sqrt[p]{A}) = 0$$

è risolubile per radicali lo saranno anche tutte le altre. Ma questa equazione ha per ipotesi almeno una radice x_1 esprimibile per radicali talchè il teorema enunciato è certamente vero per le equazioni di grado n, se lo è per le equazioni di grado inferiore (divisore di n). E poichè per le equazioni di grado primo il teorema sussiste, essa è vero in generale c. d. d.

§. 79. — **Aggiunta di una radice di un' equazione ausiliaria di grado primo.** Nelle ricerche fondamentali del §. 75 abbiamo esaminato l'abbassamento che può prodursi nel grado di un' equazione $f(x) = 0$ per l'aggiunta di **tutte** le radici di un equazione ausiliaria $\varphi(y) = 0$. Qui vogliamo esaminare ciò che accade quando si aggiunge una radice di un' equazione ausiliaria. Però ci limiteremo al caso che basta pel nostro scopo, in cui si trovino soddisfatte le condizioni seguenti e cioè: 1°. La proposta $f(x) = 0$ sia un' equazione **normale**; 2°. L'equazione ausiliaria sia irriducibile e di grado primo p. Si osserverà che la prima condizione non è veramente una limitazione perchè al problema di risolvere un' equazione qualsiasi

$f(x)=0$ si può sostituire quello relativo alla sua risolvente di Galois, che è un' equazione normale.

Ciò premesso, supponiamo che per l'aggiunta della radice y_1 dell' ausiliare irriducibile

$$\varphi_p(y)=0$$

colle radici $y_1, y_2 \dots\dots y_p$,

il gruppo di Galois della equazione normale

$$f(x)=0$$

scende da G al sottogruppo G_1 d'indice q in G. Se prendiamo una funzione razionale

$$\Psi(x_1, x_2 \dots\dots x_n)$$

delle radici della proposta, il cui sottogruppo numerico sia G_1, per essere l'equazione normale, potremo anche esprimere

$$\Psi(x_1, x_2 \dots\dots x_n)$$

per una sola radice sia

$$\Psi(x_1, x_2 \dots\dots x_n) = \Phi(x_1),$$

e la Φ stessa sarà razionalmente nota dopo l'aggiunta di y_1 e avremo quindi

$$\Phi(x_1) = \Theta(y_1)$$

essendo Θ funzione razionale intera di grado $p-1$ al massimo. Se colla funzione $\Phi(x_1)$ costruiamo la risolvente della proposta

$$(1) \qquad F_0(z)=0$$

(il cui grado q sarà l'indice ossia S_1 in S) avremo

$$F_q(\Theta(y_1)) = 0,$$

onde per la irreducibilità della $\varphi_p(y) = 0$ si conclude che

$$(2) \qquad \Theta(y_1),\ \Theta(y_2) \cdots\cdots \Theta(y_p)$$

sono altrettante radici della (1). Questi p valori sono tutti distinti fra loro(*) e razionalmente esprimibili per le x cioè p. e. per x_1. Ne segue che se al campo di razionalità altura le per l'equazione $\varphi_p(y) = 0$ aggiungiamo x_1 il gruppo di $\varphi_p(y) = 0$ scende all'identità che è la sola sost.ne che lasci invariati i singoli valori (2) e però le y sono razionalmente esprimibili per la x_1, cioè l'ausiliaria $\varphi_p(y) = 0$ non è che una risolvente della proposta. Ma allora, essendo p il suo grado, è anche $= p$ l'indice del sottogruppo S_1 cui scende S per l'aggiunta

---

(*) Se tutti i valori (2) uguali al primo fossero

$$\Theta(y_1) = \Theta(y_2) = \cdots\cdots = \Theta(y_p)$$

Applicando a queste relazioni le sostituzioni del gruppo transitivo di Galois per la $\varphi_p(y) = 0$ si concluderebbe che i p valori (2) sarebbero r ad r uguali e però $r = 1$ o $r = p$. Ma se $\Theta(y_1) = \Theta(y_2) = \cdots\cdots = \Theta(y_p)$ allora sarebbe $\Theta(y_1) = \Phi(x_1)$ razionalmente noto nel campo primitivo. Dunque $r = 1$ c. d. d.

di y_1 (§§ 63-66). Dunque:

Se per l'aggiunta di una radice di un'equazione ausiliaria irriducibile di grado primo p il gruppo dell'equazione normale $f(x)=0$ scende da G a G_1, sarà G_1 sottogruppo (*) d'indice $=p$ in G e l'equazione ausiliaria non sarà altro che una ordinaria risolvente costruita con una funzione razionale y_1 delle radici della proposta invariabile pel sottogruppo numerico G_1. È chiaro che il teorema vale anche per una equazione non normale come si vede sostituendo alla proposta la sua risolvente di Galois.

Supponiamo ora che il campo di razionalità sia reale e l'equazione normale abbia una e quindi tutte le radici reali; allora ogni ausiliare $\varphi_p(y)=0$ irriducibili di grado primo, di cui la conoscenza di una radice abbassi il gruppo della proposta, avrà essa stessa tutte le radici reali, perchè esprimibili razionalmente con coefficienti reali per le radici reali di $f(x)=0$. Dunque:

(*) Beninteso in generale non invariante.

Se per l'aggiunta di una radice d'una equazione ausiliaria irriducibile di grado primo il gruppo di una equazione normale a radici reali, in un campo reale di razionalità, viene abbassato, anche l'ausiliare avrà certamente tutte le radici reali.

§. 80. — Caso irriducibile della equazione cubica. Come è noto, nella formula Cardanica

$$x = \sqrt[3]{-\frac{p}{2} + \sqrt{\frac{p^2}{4} + \frac{q^3}{27}}} + \sqrt[3]{-\frac{p}{2} - \sqrt{\frac{p^2}{4} + \frac{q^3}{27}}}$$

per la risoluzione della equazione cubica

$$x^3 + px + q = 0,$$

quando le tre radici sono reali, si ha il così detto caso irriducibile. Allora essendo

$$-\frac{p^2}{4} + \frac{q^3}{27} < 0 \quad (*),$$

l'estrazione di radice cubica porta sopra quantità immaginarie ed ogni tentativo si riconduce i radicandi a forma reale, senza ricorrere alle formole trigonometriche

---

(*) Indicando con Δ il discriminante si ha:

$$\Delta = -(4q^3 + 27p^2).$$

(trisezione dell'angolo), riconduce alla equazione stessa. Il teorema dimostrato alla fine del § precedente ci dimostra appunto come ogni tale tentativo debba necessariamente riescir vano.

L'equazione cubica, appena aggiunto nel caso che ora consideriamo, il radicale reale $\sqrt{A}$, diventa una equazione normale (a gruppo G_3) con radici reali. Brafacilmente dimostriamo che per un'equazione normale di grado impari n a coefficienti reali non può mai prodursi un abbassamento del suo gruppo coll'aggiunta di quanti si vogliono radicali reali. E invero l'aggiunta di un radicale reale

$$\sqrt[p]{A}$$

di indice primo equivale all'aggiunta di una radice della equazione irriducibile (§. 76) di grado primo

$$z^p = A$$

E siccome questa, se $p > 2$, ha una sola radice reale, è impossibile, pel teorema del §. precedente, che il gruppo si abbassi. E nemmeno l'aggiunta di un radicale quadratico può abbassarlo giacchè l'ordine del gruppo non è divisibile per 2.(*)

(*) Se l'equazione è irriducibile l'ordine del suo gruppo è

In particolare dunque per tutte le equazioni abeliane irriducibili di grado impari le formole di risoluzione portano a radicali immaginarii e volendoli ridurre a forma reale si può unicamente ricorrere (V. § 73) alla divisione di un angolo noto in n parti uguali.

§. 81. — Risolventi di grado $< n$ della equazione generale di grado n.

Ritorniamo alle equazioni generali di grado n a gruppo totale $G_\pi(n)$ per esaminare la questione seguente: **Può un'equazione generale di grado n possedere risolventi di grado minore od eguale ad n?**

Per quanto sappiamo intorno alla formazione delle risolventi (§. 66), il problema enunciato equivale all'altro: **Esistono nel gruppo totale $G_\pi(n)$ sottogruppi d'indice $\leq n$?**

Sia Γ un tale sottogruppo d'indice $r \leq n$ e formiamo la risolvente con una funzione razionale delle radici della proposta numericamente invariabile per Γ. Indicando con

$$y_1 \quad y_2 \cdots\cdots y_r$$

(*) precisamente n, altrimenti un divisore di n.

le radici di questa risolvente, il loro gruppo $H = \frac{G}{\Gamma}$ (§ 67) sarà isomorfo con $\mathfrak{S}\pi(n)$, quindi all'identità in H corrisponderà un sottogruppo Σ invariante in $\mathfrak{S}\pi(n)$ ed eccettuato il caso $n = 4$, sarà Σ l'identità, ovvero il gruppo alterno. Ora se supponiamo dapprima $r < n$, il primo caso non può darsi perchè allora l'isomorfismo fra $\mathfrak{S}\pi(n)$, e H sarebbe che dire che H è al massimo d'ordine $\pi(r) < \pi(n)$. Dunque Σ sarà allora il gruppo alterno e perciò y una funzione semisimmetrica (a due valori), onde concludiamo:

L'equazione generale di grado n, eccettuato il caso $n = 4$, non possiede altra risolvente di grado $< n$ all'infuori di quella di secondo grado $y^2 = \Delta$.

È chiaro poi che anche ridotto, coll'estrazione della radice quadrata di Δ, il gruppo alterno, il gruppo dell'equazione, non si può costruire a causa della semplicità di questo gruppo, alcuna risolvente di grado $< n$.

Ma il caso $n = 4$ fa realmente eccezione poichè il gruppo totale $\mathfrak{S}_{24}$ possiede (tre) sottogruppi dell'ottavo ordine e quindi l'equazione generale di quarto grado ammette una risolvente cubica. Ed è appunto su questa circostanza che si fondano i metodi di risoluzione della equazione di 4° grado.

Così indicate con $x_1\ x_2\ x_3\ x_4$ le radici della equazione generale di 4° grado.

$$(2) \qquad x^4 + a x^3 + b x^2 + c x + d = 0,$$

è una funzione a tre valori la seguente:

$$y_1 = x_1 x_2 + x_3 x_4$$

e gli altri due valori sono

$$y_2 = x_1 x_3 + x_2 x_4$$
$$y_3 = x_1 x_4 + x_2 x_3$$

invertendosi

$$y_1 + y_2 + y_3 = b, \quad \Sigma y_1 y_2 = ac - 4d$$
$$\Sigma y_0 y_1 y_2 = c^2 + d(a^2 - 4b)$$

la corrispondente risolvente di 3° grado si scrive

$$(3) \qquad y^3 - b y^2 + (ac - 4a) y + d(4b - a^2) - c^2 = 0.$$

Abbiamo qui notato esplicitamente la forma di questa risolvente per poter stabilire il criterio onde riconoscere se una data equazione di 4° grado è risolubile per radicali quadratici. In tale ipotesi avremo l'equazione cubica (3) dovrà risolversi nella stessa guisa e però dovrà possedere una radice razionale. Se ne concluderà: L'equazione di 4° grado è risolubile per radicali quadratici solo quando la risolvente cubica (3) possiede una radice razio

male. Così per es. se $a = c = 0$ la (2) è biquadratica e la (3) possiede la radice razionale $y = b$.

§ 82. — **Risolvente di grado n della equazione di grado n.** Veniamo ora ad esaminare se un'equazione generale di grado n può possedere una risolvente di grado n. Ogni trasformata di Tschirnhaus alla proposta è appunto una risolvente di grado n, ma, prescindendo di questo caso ovvio, ne dimostreremo:

L'equazione generale di grado n non possiede alcuna risolvente di grado n che non sia una semplice trasformata di Tschirnhaus, il caso $n = 6$ fa però eccezione.

Sia per $n = 6$ si avvia un'eccezione resulta subito dal fatto che il gruppo lineare totale Γ sopra 6 elementi (§. 38) è appunto di ordine $= 120$ e nel gruppo totale $G_{6!}$ (6) ha quindi l'indice 6. Una risolvente dell'equazione di 6° grado costruito con una funzione razionale delle sei radici invariante per Γ è quindi appunto di 6° grado senza essere una trasformata di Tschirnhaus della proposta.

Per dimostrare il nostro teorema, cominciamo dall'osservare che il gruppo H sulle n radici

$$y_1\ y_2 \cdots\cdots y_n$$

della risolvente dovrà essere, per quanto già si è detto al §. precedente, oloedricamente isomorfo(*) col gruppo totale $G_{\Pi(n)}$ sulle n lettere

$$x_1\ x_2 \cdots\cdots x_n;$$

quindi H sarà il gruppo totale sulle $\underline{n}$ y. Se g è una sostituzione di G, h la corrispondente in H, avranno g, h eguale periodo e a due sostituzioni simili g, g' in G corrisponderanno due sostituzioni simili h, h' simili in H(**).
Ora ad una trasposizione in G dovrà corrispondere una sostituzione a periodo 2 in H cioè un prodotto di trasposizioni e se supponiamo che ad una determinata trasposizione in G corrisponda un prodotto di $\underline{r}$ trasposizioni in H, ad ogni altra trasposizione in G dovrà corrispondere un prodotto di $\underline{r}$ trasposizioni in H. Perciò dovrà il numero delle trasposizioni su $\underline{n}$ lettere cioè: $\frac{n(n-1)}{2}$ eguagliare il nu-

---

(*) Altrimenti y_1 sarebbe simmetrica o semisimmetrica.

(**) Invero se $g' = g_1^{-1} g g_1$ e a g_1 corrisponde h_1 a $g_1^{-1} g g_1$ corrisponderà $h_1^{-1} h h_1 = h'$.

mero ai prodotti distinti di r trasposizioni sopra n lettere; quest'ultimo numero è dato da(*)

$$\frac{n(n-1)\cdots\cdots(n-2r+1)}{1.2.3\ldots r.2^r}$$

e però dovremo avere

$$\frac{n(n-1)}{2}=\frac{n(n-1)\cdots\cdots(n-2r+1)}{1.2.3\ldots r.2^r}$$

cioè, per $r \geq 1$.

$$(n-2)(n-3)\cdots\cdots(n-2r+1)-2^{r-1}\Pi(r)=0.$$

Ora se supponiamo $r>3$ questa equazione per n non ha soluzioni intere perchè posto

$$f(x)=(x-r)(x-3)\cdots\cdots(x-2r+1)-2^{r-1}\Pi(r)$$

si ha $\quad f(2r)=\Pi(r)\{(2r-2)(2r-3)\cdots\cdots(r+1)-2^{r-1}\}>0$

(*) Indicando con $\Psi(r)$ questo numero ed osservando che aggiungendo ad un prodotto di $r-1$ trasposizioni una trasposizione si ottengono tutti i prodotti di r trasposizioni, ciascuno ripetuto r volte, otteniamo

$$\Psi(r)=\frac{(n-2r+2)(n-2r+1)}{2.r}\Psi(r-1)$$

indi

$$\Psi(r-1)=\frac{(n-2r+4)(n-2r+3)}{2.(r-1)}\Psi(r-2)$$

[illegible] dicando coll'osservare che $\Psi(r)=\frac{n(n-1)}{2}$ segue appunto la formula del testo

e a più forte ragione $f(n) > 0$ per $n > 2r$; se poi $1 < n < 2r$ è

$$f(n) = -2^{n-1}\Pi(n) < 0.$$

D'altronde vennero per $n = 2$ l'equazione precedente fra una radice intera e solo per $n = 3$ abbiamo la radice intera $n = 0$. Dunque intanto: **Eccettuato il caso $n = 6$ ad ogni trasposizione in $\mathfrak{S}$ dovrà corrispondere una trasposizione in H.**

Se ben significare la corrispondenza di due sostituzioni g, h scriviamo $g \equiv h$ e supponiamo che sia

$$(x_1 x_n) \equiv (y_a y_b), \quad (x_1 x_3) \equiv (y_c y_a)$$

avremo

$$(x_1 x_2 x_3) = (x_1 x_2)(x_1 x_3) \equiv (y_a y_b)(y_c y_a)$$

e però uno degli indici c, d dovrà eguagliare o a o b. Senza alterare la generalità potremo supporre $d = a$ e avremo

$$(x_1 x_2) \equiv (y_a y_b), \quad (x_1 x_3) \equiv (y_a y_c)$$

Ora se $(x_1 x_H) \equiv (y_d y_e)$, dovrà similmente uno dei due indici d, e essere uguale ad un indice di $(y_a y_b)$ e ad uno di $(y_a y_c)$ quindi per esempio sarà $e = a$(*). Così continuando

---

(*) Non può aversi $(x_1 x_H) \equiv (y_b y_c)$ perchè

$(y_b y_c) = (y_a y_b)(y_a y_c)(y_a y_b)$ corrisponde invece a

$(x_1 x_2)(x_1 x_3)(x_1 x_2) = (x_2 x_3)$

concluderemo che si possono disporre le y_i in tale ordine e si ha (cangiando gli indici alle y)

$$y_1\ y_2 \ldots\ldots y_n$$

per modo che si abbia

$$(x_1\ x_2) \equiv (y_1\ y_2) \qquad r = 2, 3, \ldots\ldots n$$

quindi anche $(x_n\ x_2) \equiv (y_n\ y_1)$

In tal caso adunque ogni sostituzione di H si deduce da la corrispondente di $\mathfrak{G}$ semplicemente cangiando le x nelle y. Ma allora alle $\Pi(n-1)$ sostituzioni di H che lasciano fermo y_1 corrispondono le $\Pi(n-1)$ sostituzioni di $\mathfrak{G}$ che lasciano fermo x_1 e però y_1 è razionalmente esprimibile per x_1, cioè la sostituzione risolvente non è che un'ordinaria trasformata di Tschirnhaus della proposta c. d. d.

Il nostro risultato può anche esprimersi dicendo: Il gruppo totale di n lettere, per $n = 6$, non può farsi in corrispondenza di isomorfismo ed ibedrico con se stesso altrimenti che cangiando la denominazione alle lettere, laddove per $n = 6$ esiste un'altra tale corrispondenza essenzialmente diversa.

§. 23.- **Equazioni di grado primo risolubili.** Abbiamo stabilito al §. 11 il criterio di Galois per la risolubilità di una equazione per radicali, consistente in ciò che il suo gruppo deve avere per grado il complemento dei numeri primi. Nel caso delle equazioni di **grado primo** si può dare al criterio stesso una altra forma, assegnata ancora da Galois, di cui ora cominciamo ad occuparci.

Sappiamo che un'equazione di grado primo p **irriducibile** sia solubile per radicali; allora il suo gruppo (§. 3.4 o s.s.) dovrà essere il gruppo metaciclico

$$\mathfrak{G}_p\,(p-1)$$

sopra le p radici $x_0, x_1, x_2, \ldots\ldots, x_{p-1}$

convenientemente ordinate, ovvero un suo sottogruppo di ordine p^s. Ma siccome nel gruppo $\mathfrak{G}_p\,(p-1)$ e a fortiori in ogni suo sottogruppo, esiste la sola identità che non muta alcuna determinata radici ne deduciamo:

Se un'equazione irriducibile di grado primo è risolubile per radicali, prese due radici qualsiasi le altre si esprimeranno razionalmente per esse.

Viceversa supponiamo che un'equazione irriducibile di

grado primo p gode della proprietà che per due radici fisse p.e. x_0, x_1 si esprimano razionalmente tutte le altre e dimostriamo che il suo gruppo sarà il gruppo metaciclico (o un sottogruppo) e però l'equazione sarà risolubile per radicali. È infatti l'ordine del gruppo $\mathfrak{G}$ dell'equazione sarà dato da $m = kp$

e poichè la sola identità in $\mathfrak{G}$ lascia ferme x_0, x_1, sarà m eguale al massimo al numero dei sistemi di posti che possono occupare $x_0 x_1$ cioè a $p(p-1)$; dunque

$$k < p-1$$

Ora $\mathfrak{G}$ contiene certamente una sostituzione S di periodo p (ciclica nelle p radici), quindi il gruppo ciclico

$$\Gamma_p = (1, S, S^2 \ldots\ldots S^{p-1}).$$

Se con A indichiamo una sostituzione di $\mathfrak{G}$ fuori di Γ i p seguenti sono le p^2 sostituzioni

$$S^a A S^b \quad \{a, b = 0, 1, 2 \ldots\ldots p-1,$$

queste appartengono tutte a $\mathfrak{G}$, onde, essendo $p^2 > m$, ve ne saranno delle eguali, poniamo

$$S^a A S^b = S^{a'} A S^{b'}$$

con $\qquad a \neq a', \quad b \neq b' \ (\text{ma } a \neq b)$

se deduciamo $\qquad A^{-1} S^{a'-a} A = S^{b'-b}$

e determinando il numero $\leq$ delle coniugate

$$(\lambda - \alpha) r \equiv 1 \pmod{p},$$

ne segue $(U^{-1} S^{\lambda-\alpha} U)^r = U^{-1} S U = S^{(\lambda-\beta) r}$;

dunque U, trasformando S in una potenza di S, appartiene al gruppo metaciclico c. d. d.

Possiamo quindi enunciare il teorema di Galois:

Affinchè un'equazione irriducibile di grado primo sia risolubile per radicali è necessario e sufficiente che tutte le sue radici possano esprimersi razionalmente per due di essa.

Segue di qui che se il campo di razionalità è reale l'equazione avrà tutte le radici reali ovvero una sola radice reale. Dopo di ciò è facilissimo formare a piacere esempi relativi di razionalità, delle equazioni irriducibili di grado primo p qualsiasi insolubili per radicali. Così p. e. l'equazione

$$f(x) = x^p + m q x^2 - q = 0$$

essendo p, q numeri primi qualsiansi ed m un intero > 1 è irriducibile e trascendendo una radice reale positiva e due negative (*) è insolubile per radicali se $p > 3$.

(*) In la regola dei segni di Cartesio essa non può avere in

§. 84. — **Risolvente di Lagrange.** — Il criterio che abbiamo sopra stabilito per decidere se un'equazione di grado primo è solubile per radicali può trasformarsi in guisa da dargli anche un valore pratico si da poter riconoscere, sopra una data equazione, se essa è o no risolubile.

Perciò costruiamo una funzione razionale delle p radici

$$x_0\, x_1\, x_2 \cdots\cdots x_{p-1}$$

della proposta $f(x)=0$ che rimanga numericamente invariata per tutte e sole le sostituzioni del gruppo rivetaciclico $G_{p(p-1)}$; essa avrà allora $n = 1.2.3\cdots\cdots(p-2)$ valori numericamente distinti che saranno radici di una equazione (risolvente) razionalmente costruibile:

$$(y-y_0)(y-y_1)\cdots\cdots(y-y_n)=0$$

Questa dicesi la **risolvente di Lagrange** della equazione proposta.

Ora se la $f(x)=0$ è risolubile per radicali, la risolvente di Lagrange avrà una radice razionale perchè il suo gruppo

---

Sarà più radici reali di quelle qui indicate; ma questo è ne effettivamente perchè.

$$f(-\infty)<0,\ f(-1)>0,\ f(0)<0,\ f(1)>0.$$

sarà metaciclico e per ciò simile a $G_{\varphi(p-1)}$ (o ad un suo sottogruppo). Se τ è una sostituzione che trasforma $G_{\varphi(p-1)}$ nel gruppo di $f(x)=0$, la radice y_τ della risolvente di Lagrange, dedotta da y_1 colla sostituzione τ sulle x, sarà razionalmente nota.

Viceversa se una radice y_τ della risolvente di Lagrange è razionale, il gruppo della equazione conterrà solo sostituzioni che la lasciano invariata e però sarà il gruppo metaciclico $\tau^{-1} G_{\varphi(p-1)} \tau$ ovvero un suo sottogruppo, onde l'equazione sarà risolubile per radicali.

Abbiamo dunque il teorema: **La condizione necessaria e sufficiente affinchè una equazione di grado primo sia risolubile per radicali è che la sua risolvente di Lagrange abbia una radice razionale.**

§. 85.— **Il problema della divisione del circolo in m parti uguali.** Andiamo ora ad applicare le teorie generali che abbiamo svolto fin qui al classico esempio delle equazioni per la divisione del circolo in m parti uguali per far conoscere, almeno nei

questo radici e con

$$a_1\, a_2 \ldots\ldots\ldots a_{p^{r-1}(p-1)}$$

indichiamo i numeri di un sistema completo di resti (mod p^r) esclusi i divisibili per p, tutte le radici della (3) saranno

$$\varepsilon^{a_1},\ \varepsilon^{a_2},\ \varepsilon^{a_3} \ldots\ldots \varepsilon^{a_{p^{r-1}(p-1)}}$$

Ora è ben noto (*) che esistono radici primitive g del numero p^r, tali cioè che ponendo per brevità $\nu = p^{r-1}(p-1)$, le ν potenze di g

$$1,\ g,\ g^2 \ldots\ldots g^{\nu-1}$$

sono fra loro incongrue (mod p^r) e allora se ordiniamo le ν radici della (3) così:

$$(4) \qquad \varepsilon,\ \varepsilon^g,\ \varepsilon^{g^2} \ldots\ldots\ldots \varepsilon^{g^{\nu-1}}$$

vediamo che l'equazione (3) è Abeliana e le sue radici formano un unico periodo.

§. 86. – Irreducibilità dell'equazione

$$\frac{x^{p^r}-1}{x^{p^{r-1}}-1} = 0$$

Dimostriamo ora che: **Nel campo assoluto di razionalità l'equazione (3) è irreducibile.** Nel caso dell'equazione

---

(*) V.i p.e. Dirichlet-Dedekind. Zahlen = Theorie Suppl. V.

(5) $x^{p-1} + x^{p-2} + \dots\dots x + 1 = 0$ abbiamo dato al § 74 la dimostrazione di Eisenstein, la quale facilmente si estende anche al caso più generale della equazione (3). Qui faremo conoscere un'altra semplice dimostrazione dovuta a Kronecker. Se supponiamo la funzione (3) $f(x)$ riducibile essa dovrà scindersi (§ 58) nel prodotto di due altre funzioni $\varphi(x)\ \psi(x)$ a coefficienti interi e col primo coefficiente = 1. Ora se in

$$f(x) = \varphi(x)\ \psi(x)$$

poniamo $x = 1$, essendo $f(1) = p$, ne deduciamo

$$p = \varphi(1) \cdot \psi(1),$$

per cui dei due numeri interi $\varphi(1)$, $\psi(1)$ uno sarà eguale a ± 1 e l'altro a $\pm p$; sia

$$\varphi(1) = \pm 1 \quad , \quad \psi(1) = \pm p.$$

Ora, le radici $\varepsilon^{a_1}\ \varepsilon^{a_2} \dots\dots \varepsilon^{a_\nu}$ di $f(x) = 0$ appartenendosi fra $\varphi(x)$ e $\psi(x)$, avremo certamente

$$\varphi(\varepsilon^{a_1})\,\varphi(\varepsilon^{a_2}) \dots\dots \varphi(\varepsilon^{a_\nu}) = 0$$

e però l'equazione

$$\varphi(x^{a_1})\,\varphi(x^{a_2}) \dots\dots \varphi(x^{a_\nu}) = 0$$

avendo tutte le radici di $f(x) = 0$, dovremo avere

$$\varphi(x^{a_1})\,\varphi(x^{a_2}) \dots\dots \varphi(x^{a_\nu}) = f(x)\,\theta(x),$$

dove $\theta(x)$ è ancora un polinomio razionale in

ro in x a coefficienti interi. Ma se in quest'ultima formola poniamo $x=1$, ne dedurremmo l'eguaglianza assurda

$$1 = p\,\theta(1).$$

Dimostrata l'irreducibilità di $f(x)=0$, segue dalle osservazioni premesse che il gruppo dell'equazione è il gruppo ciclico d'ordine $\quad V = p^{r-1}(p-1)$

generato dalle potenze della sostituzione ciclica

$$S = (\varepsilon, \varepsilon^g, \varepsilon^{g^2}, \ldots, \varepsilon^{g^{V-1}}).$$

Per la risoluzione di questa equazione, oltre l'estrazioni di radicali di indici corrispondenti ai divisori primi di $p-1$ si richiede l'estrazione di $r-1$ radicali di indice $= p$, cioè l'iscrizione nel circolo del poligono regolare di p^r lati, appena $r>1$, non si può più eseguire colla riga e col compasso.(*)

(*) Perchè un problema geometrico (determinato) sia risolubile colla riga e col compasso occorre e basta che l'equazione (irriducibile) in cui il problema vien tradotto, sia risolubile con soli radicali quadrati. Ciò accade soltanto (§. 76) se l'ordine del gruppo è una potenza del 2, nel qualcaso anche il grado della equazione sarà necessariamente una potenza del 2.

§. 5. - **I periodi di Gauss.** Ed ora andiamo ad occuparci più specialmente del caso $r=1$, cioè dell'equazione

$$(5) \quad x^{p-1} + x^{p-2} + \cdots\cdots + x + 1 = 0,$$

la cui risoluzione equivale all'iscrizione nel circolo del poligono regolare di p lati. Noi ci proponiamo di costruire effettivamente per questo caso le diverse risolventi, di cui i teoremi generali ci fanno riconoscere l'esistenza. Se indichiamo con ε una qualunque radice della (5), con g una radice primitiva (mod p), il gruppo della (5) è costituito dalle $p-1$ potenze della sostituzione ciclica

$$S = (\varepsilon, \varepsilon^g, \varepsilon^{g^2}, \cdots\cdots \varepsilon^{g^{p-2}}).$$

Per costruire una risolvente della (5) dobbiamo prendere un sottogruppo Γ del gruppo

$$\mathfrak{G}_{p-1} = (1, S, S^2, \cdots\cdots S^{p-2})$$

ed assumere una funzione razionale delle radici della (5) invariabile per tutte e sole le sostituzioni di Γ. Se indichiamo con S^e la minima potenza di S che figura in Γ, tutte le altre avranno esponenti multipli di e (*), onde risulta che e sarà un divisore di $p-1$, poniamo

---

(*) Sia invero S^m una tale potenza: se r è il minimo resto positivo di m (mod e) dovrà

$$p-1 = e f$$

ed avremo

$$S^e = (\varepsilon, \varepsilon^{g^e}, \varepsilon^{g^{2e}} \dots \varepsilon^{g^{(f-1)e}}) \times$$
$$\times (\varepsilon^g, \varepsilon^{g^{e+1}}, \varepsilon^{g^{2e+1}} \dots \dots \varepsilon^{g^{(f-1)e+1}}) \times$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\times (\varepsilon^{g^{e-1}} \varepsilon^{g^{2e-1}} \dots\dots\dots \varepsilon^{g^{ef-1}})$$

Ora una funzione invariabile per la sostituzione S^e, quindi pel gruppo Γ, è data semplicemente da

$$\eta_0 = \varepsilon + \varepsilon^{g^e} + \varepsilon^{g^{2e}} + \dots\dots + \varepsilon^{g^{(f-1)e}}$$

e i valori distinti (come ora dimostreremo) che essa assume per le sostituzioni di G sono gli e seguenti:

$$(6) \quad \begin{cases} \eta_0 = \varepsilon + \varepsilon^g + \varepsilon^{g^e} + \dots\dots + \varepsilon^{g^{(f-1)e}} \\ \eta_1 = \varepsilon^g + \varepsilon^{g^{e+1}} + \varepsilon^{g^{2e+1}} + \dots\dots + \varepsilon^{g^{(f-1)e+1}} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ \eta_{e-1} = \varepsilon^{g^{e-1}} + \varepsilon^{g^{2e-1}} + \varepsilon^{g^{3e-1}} + \dots\dots + \varepsilon^{g^{fe-1}} \end{cases}$$

Questi diconsi i **periodi di Gauss** e facilmente dimostriamo anzitutto che essi sono numericamente diversi, poichè supposto $\eta_k = \eta_{k+e}$ cioè

$$\varepsilon^{g^k} + \varepsilon^{g^{k+e}} + \dots\dots + \varepsilon^{g^{k+(f-1)e}} = \varepsilon^{g^k} + \varepsilon^{g^{k+e}} + \dots\dots \varepsilon^{g^{k+(f-1)e}}$$

$$n = q e + r$$

anche $S^{-qe} \cdot S^n = S^r$ sarà in Γ, onde $r = 0$.

riducendo ciascun esponente g^μ al suo minimo resto positivo (mod p) e dividendo la relazione per ε, si avrebbe un'equazione con coefficienti interi di grado $p-2$ al massimo cui soddisferebbe ε. E poichè questa equazione non è identica, ne seguirebbe che la (5) sarebbe riducibile.

Gli e periodi η di Gauss sono radici di una risolvente di grado e che indicheremo con

$$(7) \qquad F_e(\eta) = (\eta - \eta_0)(\eta - \eta_1)\cdots(\eta - \eta_{e-1}).$$

Questa risolvente ha il primo coefficiente $=1$ e gli altri, in ordine ai teoremi generali sono numeri razionali. Ma di più vogliamo qui dimostrare che essi sono numeri interi. Ciò resulta come caso particolare dal teorema generale seguente:

Ogni funzione razionale intera a coefficienti interi delle radici della (5) numericamente invariabile per le sostituzioni del gruppo G_{p-1} è eguale ad un numero intero(*). E invero a

---

(*) Questo teorema non è poi altro che un caso particolare dell'altro che dice: Se un'equazione $F(x)=0$ ha per primo coefficiente 1 e gli altri interi, qualunque funzione razionale in-

una tale funzione $\Phi(\varepsilon, \varepsilon^g, \varepsilon^{g^2} \ldots\ldots \varepsilon^{g^{p-2}})$ si potrà in primo luogo porre sotto la forma

$$\Phi = a_0 + a_1\varepsilon + a_2\varepsilon^g + a_3\varepsilon^{g^2} + \ldots\ldots a_{p-1}\varepsilon^{g^{p-2}},$$

le a_i essendo numeri interi, indi osservando che

$$\varepsilon + \varepsilon^g + \varepsilon^{g^2} + \ldots\ldots + \varepsilon^{g^{p-2}} = -1$$

sotto l'altra

$$\Phi = \alpha_0\varepsilon + \alpha_1\varepsilon^g + \alpha_2\varepsilon^{g^2} + \ldots\ldots + \alpha_{p-2}\varepsilon^{g^{p-2}}$$

colle α num i interi. Questa ci darà la forma della Φ. Questa forma normale è unica perchè da

$$\alpha_0\varepsilon + \alpha_1\varepsilon^g + \ldots\ldots + \alpha_{p-2}\varepsilon^{g^{p-2}} = \beta_0\varepsilon + \beta_1\varepsilon^g + \ldots + \beta_{p-2}\varepsilon^{g^{p-2}},$$

col processo già sopra adoperato seguirebbe che la (5) è riducibile.

Ora se la Φ è numericamente invariabile per la S, avremo

$$\alpha_0\varepsilon + \alpha_1\varepsilon^g + \alpha_2\varepsilon^{g^2} + \ldots + \alpha_{p-2}\varepsilon^{g^{p-2}} =$$
$$= \alpha_0\varepsilon^g + \alpha_1\varepsilon^{g^2} + \alpha_2\varepsilon^{g^3} + \ldots + \alpha_{p-2}\varepsilon,$$

onde segue $\alpha_0 = \alpha_1 = \alpha_2 = \ldots\ldots\ldots = \alpha_{p-2}$,

quindi

$$\Phi = \alpha_0(\varepsilon + \varepsilon^g + \ldots\ldots + \varepsilon^{g^{p-2}}) = -\alpha_0$$

ciò che dimostra il teorema.

---

tera a coefficienti interi delle sue radici, razionalmente nota, è equale ad un numero intero.

§. 88.— La risolvente $F_e(\eta) = 0$. La sostituzione

$$S = (\varepsilon, \varepsilon^g, \varepsilon^{g^2} \ldots \varepsilon^{g^{p-2}})$$

produce sui periodi η di Gauss la sostituzione ciclica

$$U = (\eta_0 \eta_1 \eta_2 \ldots \eta_{e-1}).$$

Dunque il gruppo della risolvente $F_e(\eta) = 0$ (§. 87) è il gruppo ciclico

$$G_e = (1, U, U^2, \ldots U^{e-1});$$

la $F_e(\eta) = 0$ è quindi un'equazione Abeliana irriducibile a gruppo ciclico. Per risolverla occorre aggiungere la radice primitiva della unità d'ordine e

$$\rho = \cos\frac{2\pi}{e} + i \operatorname{sen}\frac{2\pi}{e}$$

ed estrarre inoltre un radicale d'indice e.

Risolta la $F_e(\eta) = 0$ il gruppo G_{p-1} della proposta si riduce al sottogruppo Γ_f formato dalle potenze S^e. Ogni funzione razionale delle radici della proposta invariabile per S^e è quindi razionalmente esprimibile per i periodi

$$\eta_0, \eta_1 \ldots \eta_{e-1}.$$

Ma nel corso nostro possiamo vie più precisare questa proprietà dimostrando il teorema:

Ogni funzione razionale intera a coefficienti interi di $\varepsilon, \varepsilon^g, \varepsilon^{g^2} \ldots \varepsilon^{g^{p-2}}$ numericamente invariabile per la S^e si può esprime

se per una funzione lineare intera ed omogenea dei periodi $\eta_0 \eta_1 \ldots \eta_{e-1}$ con coefficienti interi.

Poniamo infatti questa funzione Φ sotto la forma normale

$$\Phi = \alpha_0 \varepsilon + \alpha_1 \varepsilon^g + \alpha_2 \varepsilon^{g^2} + \ldots\ldots + \alpha_{p-2} \varepsilon^{g^{p-2}} = \sum_{r=0}^{r=p-2} \alpha_r \varepsilon^{g^r} ;$$

abbiamo per ipotesi

$$\sum_r \alpha_r \varepsilon^{g^r} = \sum_r \alpha_r \varepsilon^{g^{e+r}}$$

onde

$$\alpha_0 = \alpha_e = \alpha_{2e} = \ldots\ldots$$
$$\alpha_1 = \alpha_{e+1} = \alpha_{2e+1} = \ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

e però

$$\Phi = \alpha_0 \eta_0 + \alpha_1 \eta_1 + \ldots\ldots + \alpha_{e-1} \eta_{e-1}$$

le α essendo numeri interi c. d. d.

In particolare segue dal nostro teorema che il prodotto di due o più periodi η uguali o diversi sarà esprimibile sotto questa forma.

L'equazione $F_e(\eta) = 0$ essendo Abeliana basterà conoscerne una radice α per conoscerle tutte. Supposta nota una tale radice α, si può domandare a quale dei periodi η è eguale; ma siccome con ε abbiamo indicato una

na qualunque delle radici della (5) possiamo senz'altro supporre $\eta_{i,0} = a$. Si troveranno allora le altre radici osservando che, pel teorema precedente, si ha

$$\begin{cases} \eta_{i,0}^2 = a_0 \eta_{i,0} + a_1 \eta_{i,1} + \cdots a_{e-1} \eta_{i,e-1} \\ \eta_{i,0}^3 = b_0 \eta_{i,0} + b_1 \eta_{i,1} + \cdots b_{e-1} \eta_{i,e-1} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \eta_{i,0}^{e-1} = l_0 \eta_{i,0} + l_1 \eta_{i,1} \cdots l_{e-1} \eta_{i,e-1} \end{cases}$$

le $a, b, \ldots l$ essendo numeri interi. Aggiungendo a queste equazioni l'altra

$$-1 = \eta_{i,0} + \eta_{i,1} + \cdots + \eta_{i,0-1},$$

si potranno risolvere queste $e-1$ equazioni lineari rispetto ad $\eta_{i,1}, \eta_{i,2} \cdots \eta_{i,e-1}$ (*) e determinare queste in funzione razionale intera di $\eta_{i,0}$.

§. 89.— **Risolventi successive.** Fra le funzioni cui è applicabile il teorema del § precedente trova evidentemente le seguenti

$$(x - \varepsilon^{g^h})(x - \varepsilon^{g^{h+c}}) \cdots (x - \varepsilon^{g^{h+(e-1)c}})$$

(*) È impossibile che il determinante delle $e-1$ equazioni lineari sia nullo, altrimenti η_0 soddisferebbe ad un'equazione di grado $e-1$ mentre la $F_e(\eta) = 0$ è irriducibile.

$i = 0, 1, 2 \cdots e-1,$

la x essendo un'indeterminata. Risolta la $F_e(\eta) = 0$, la proposta si scinde adunque in e fattori razionali di grado f, ciò che resulta del resto dalla teoria generale. Dopo di ciò basta quindi risolvere l'equazione di grado f:

$$(\beta) \quad (x-\varepsilon)(x-\varepsilon^{g^e}) \cdots (x-\varepsilon^{g^{(f-1)e}}) = 0$$

i cui coefficienti sono funzioni lineari intere a coefficienti interi dei periodi $\eta_0\ \eta_1 \cdots \eta_{e-1}$. La (β) ha per gruppo il gruppo ciclico generato dalla sostituzione

$$V = (\varepsilon, \varepsilon^{g^e} \cdots \varepsilon^{g^{(f-1)e}})$$

d'ordine f ed è quindi un'equazione Abeliana irriducibile.

Su di essa possiamo quindi procedere come sulla proposta e se f è scindibile in due fattori e', f', se ne potrà costruire una risolvente di grado e', le cui radici saranno

$$\begin{cases} \eta'_0 = \varepsilon + \varepsilon^{g^{e'e}} + \varepsilon^{g^{2e'e}} + \cdots + \varepsilon^{g^{(f'-1)e'e}} \\ \eta'_1 = \varepsilon^{g^e} + \varepsilon^{g^{(e'+1)e}} + \cdots + \varepsilon^{g^{[(f'-1)e'+1]e}} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \eta'_{e'-1} = \varepsilon^{g^{(e'-1)e}} + \varepsilon^{g^{(2e'-1)e}} + \cdots + \varepsilon^{g^{(f'e'-1)e}} \end{cases}$$

I coefficienti di questa risolvente

$$\Phi_{e'}(\eta') = (\eta' - \eta'_0)(\eta' - \eta'_1) \cdots (\eta' - \eta'_{e'-1}) = 0$$

saranno funzioni lineari intere a coefficienti interi

di $\eta_0\, \eta_1 \dots\dots \eta_{e-1}$; la $\Phi_{e'}(v_i')=0$ è un'equazione Abeliana irriducibile e gruppo ciclico, che si risolve estraendo un radicale d'indice e'. Dopo ciò sarà razionalmente noto il fattore $\quad (x-\varepsilon)(x-\varepsilon^{g^{e'e}})\dots\dots(x-\varepsilon^{g^{(f'-1)e'e}})$

della proposta; eguagliandolo a zero avremo un'equazione Abeliana a gruppo ciclico nella quale potremo procedere come nello (8) scindendo f' in due fattori $f'=e''f''$ e così via di seguito.

Se per i fattori

$$e,\ e',\ e''\dots\dots$$

prendiamo i successivi fattori primi di $p-1$ essendo

$$p-1=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\dots\dots p_r^{\alpha_r}$$

ritroviamo nuovamente il teorema alla fine del § 74. Siccome in cui i fattori primi di $p-1$ sono distribuiti nella serie $e,\ e',\ e''\dots$ è, come è chiaro, indifferente. Sarà però utile ritenere per ultimo fattore il $\underline{2}$; con ciò infatti si avrà il vantaggio che gli **ultimi** periodi da determinarsi saranno i binarii

$$\varepsilon+\varepsilon^{g^{\frac{p-1}{2}}},\ \varepsilon^{g}+\varepsilon^{g^{\frac{p-1}{2}+1}},\ \varepsilon^{g^2}+\varepsilon^{g^{\frac{p-1}{2}+2}},\dots\dots$$

ossia

$$\varepsilon+\varepsilon^{-1},\ \varepsilon^{g}+\varepsilon^{-g},\ \varepsilon^{g^2}+\varepsilon^{-g^2},\dots\dots\dots$$

i quali sono tutti reali, e reali saranno pure i periodi più [illegible]

radici che avremo prima dovuto determinare, constando di somme di due soli. Così tutte le successive risolventi saranno a radici reali e soltanto nella risoluzione dell'ultima data, resta il periodo binario $\varepsilon + \varepsilon^{-1}$, dà la ε stessa, passeremo alle radici immaginarie della proposta.

§. 90. — **Poligoni regolari inscrivibili nel cerchio colla riga e col compasso.** L'inscrizione nel cerchio del poligono regolare di un numero primo p di lati si potrà eseguire colla riga e col compasso allora soltanto che $p-1$ sia una potenza esatta del 2 (Cfr. la nota in fine al §. 86). In generale resulta dalle cose precedenti il teorema:

Perchè il poligono regolare di m lati sia costruibile geometricamente (colla riga e col compasso) è necessario e sufficiente che i fattori primi dispari di m entrino in m alla prima potenza soltanto e siano tutti della forma $p = 2^n + 1$.

Così $n = 3$, $p = 5$ dei numeri primi e i corrispondenti [illegible] dei numeri composti erano già noti nell'

tichità; colla teoria di Gauss furono noti i nuovi casi

$$p = 17,\ 257,\ 65537,\ \ldots\ldots$$

Rispetto ai numeri primi contenuti nella forma

$$p = 2^n + 1$$

è da osservarsi che n stesso deve essere una potenza del 2, cioè $n = 2^\mu$ perchè se $n = 2^\mu(2r+0)$, essendo già x^{2r+1} algebricamente divisibile per $x+1$, ne segue che $2^{2^\mu(2r+1)}+1$ ammette il fattore $2^{2^\mu}+1$. Però non tutti i numeri della forma $2^{2^\mu}+1$ sono primi, come Fermat aveva supposto. I casi noti oggidì di numeri composti di questa forma sono i quattro seguenti

$$2^{2^5}+1 \text{ (Eulero)},\quad 2^{2^6}+ \text{ (Landry)}$$

$$2^{2^{2^2}}+1 \text{ (Pervacchine)},\quad 2^{2^{2^3}}+1 \text{ (Pervacchine Lucas)}.$$

Non si conosce la legge secondo cui sono distribuiti nella serie 2^2+1 i numeri primi e nemmeno è certo se infiniti sono i numeri primi in essa contenuti.

§ 91. – Inscrizione dei poligoni regolari di 5 e 17 lati.

Fermiamoci un momento ad applicare le teorie generali ai casi $p=5$, $p=17$.

Per $p=5$ i periodi binari sono

$$\eta_0 = \varepsilon + \varepsilon^4 \qquad \eta_1 = \varepsilon^2 + \varepsilon^3$$

ed osservando che si ha:

$$\eta_0+\eta_1=-1\,,\quad \eta_0\eta_1=-1,$$

si ha subito per la risolvente di secondo grado

$$F_2(\eta)=\eta^2+\eta-1=0$$

delle cui radici una si può eguagliare a η_0 l'altra a η_1 (§. 88), poniamo

$$\eta_0=\frac{-1+\sqrt{5}}{2}\,,\quad \eta_1=\frac{-1-\sqrt{5}}{2}.$$

Trovato η_0, resta da risolversi l'equazione di secondo grado

$$(x-\varepsilon)(x-\varepsilon^4)=x^2-\eta_0 x+1=0;$$

troviamo quindi per ε

$$\varepsilon=\frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}.$$

Assumendo i radicali positivamente, si vede subito che si ha $\varepsilon=\cos\frac{2\pi}{5}+i\,\operatorname{sen}\frac{2\pi}{5}$ e la formola

$$2\cos\frac{2\pi}{5}=\eta_0=\frac{\sqrt{5}-1}{2}$$

dà una costruzione geometrica la più semplice del pentagono regolare iscritto.

Sia ora $p=17$ e scegliendo per radice primitiva $\underline{g}$ (mod 17) il $\underline{3}$ costruiamo la tabella d'indici

numero	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
indice	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

vediamo la distribuzione delle radici in periodi e formiamo i periodi di 8 termini

$$\eta_0 = \varepsilon + \varepsilon^9 + \varepsilon^{13} + \varepsilon^{15} + \varepsilon^{16} + \varepsilon^8 + \varepsilon^4 + \varepsilon^2$$
$$\eta_1 = \varepsilon^3 + \varepsilon^{10} + \varepsilon^5 + \varepsilon^{11} + \varepsilon^{14} + \varepsilon^7 + \varepsilon^{12} + \varepsilon^6,$$

gli esponenti della ε in η_0 essendo i residui, in η_1 i non residui. Scindiamo poi η_0 i due periodi minori η'_0 η'_2, corrispondenti agli indici

$$0, 4, 8, 12 \text{ per } \eta'_0$$
$$2, 6, 10, 14 \text{ per } \eta'_2$$

e similmente η_1 nei due periodi η'_1 η'_3 corrispondenti agli indici

$$1, 5, 9, 13 \text{ per } \eta'_1$$
$$3, 7, 11, 15 \text{ per } \eta'_3;$$

avremo cioè

$$\eta'_0 = \varepsilon + \varepsilon^{13} + \varepsilon^{16} + \varepsilon^4 \quad , \quad \eta'_1 = \varepsilon^3 + \varepsilon^5 + \varepsilon^{14} + \varepsilon^{12}$$
$$\eta'_2 = \varepsilon^9 + \varepsilon^{15} + \varepsilon^8 + \varepsilon^2 \quad , \quad \eta'_3 = \varepsilon^{10} + \varepsilon^{11} + \varepsilon^7 + \varepsilon^6$$

Infine scindiamo η'_0 nei due periodi

$$\eta''_0 = \varepsilon + \varepsilon^{16}$$
$$\eta''_4 = \varepsilon^{13} + \varepsilon^4.$$

Se per fissare le idee assumiamo

$$\varepsilon = \cos\frac{2\pi}{17} + i \operatorname{sen}\frac{2\pi}{17},$$

vediamo subito che i tre periodi

$$\eta_0 = 2\left(\cos\frac{2\pi}{17} + \cos\frac{4\pi}{17} + \cos\frac{8\pi}{17} + \cos\frac{16\pi}{17}\right)$$
$$\eta'_1 = 2\left(\cos\frac{6\pi}{17} + \cos\frac{10\pi}{17}\right)$$
$$\eta'_0 = 2\left(\cos\frac{2\pi}{17} + \cos\frac{8\pi}{17}\right)$$

sono positivi.

ora per costruire la risolvente di 2° grado di cui η_0 η_1 sono radici, basta osservare che si ha

$$\eta_0 + \eta_1 = -1 \qquad \eta_0 \eta_1 = H(\eta_0 + \eta_1) = -H,$$

onde la risolvente sarà

$$\eta^2 + \eta - H = 0,$$

indi

$$(\alpha) \qquad \eta_0 = \frac{\sqrt{17}-1}{2}, \qquad \eta_1 = -\frac{\sqrt{17}+1}{2}.$$

ma si ha $\eta'_0 + \eta'_2 = \eta_0$ $\quad \eta'_0 \eta'_2 = -1$

$\eta'_1 + \eta'_3 = \eta_1$ $\quad \eta'_1 \eta'_3 = -1$

e perciò η'_0, η'_2 sono le radici della equazione $\eta'^2 - \eta_0 \eta' - 1 = 0$

e η'_1 η'_3 quelle dell'altra $\eta'^2_1 - \eta_1 \eta' - 1 = 0$

onde

$$(\beta) \qquad \eta'_0 = \frac{\eta_0}{2} + \sqrt{\frac{\eta_0^2}{4} + 1}, \qquad \eta'_1 = \frac{\eta_1}{2} + \sqrt{\frac{\eta_1^2}{4} + 1},$$

In fine essendo

$$\eta''_0 + \eta''_H = \eta'_0, \qquad \eta''_0 \eta''_H = \eta'_1,$$

dedurremo

$$\eta''_0 = 2\cos\frac{2\pi}{17} = \frac{\eta'_0}{2} + \sqrt{\frac{\eta'^2_0}{4} - \eta'_1}$$

Sostituendo in questa per η'_0, η'_1 i valori (β) calcolati mediante le (α), costruiamo $\cos\frac{2\pi}{17}$ con tre successive estrazioni di radici quadrate, indi $\operatorname{sen}\frac{2\pi}{17}$ con una quarta.

§. 92. — La risolvente di 2° grado della equazione $\frac{x^p-1}{x-1}=0$.

Ritorniamo ora all'equazione generale

$$x^{p-1}+x^{p-2}+\dots\dots+x+1=0$$

Ora costruire la risolvente di secondo grado che ha per radici i periodi di $\frac{p-1}{2}$ termini:

$$\begin{cases}\eta_0=\varepsilon+\varepsilon^{g^2}+\varepsilon^{g^4}+\dots\dots+\varepsilon^{g^{p-3}}\\ \eta_1=\varepsilon^g+\varepsilon^{g^3}+\varepsilon^{g^5}+\dots\dots+\varepsilon^{g^{p-2}}\end{cases}$$

Siccome conosciamo già

$$\eta_0+\eta_1=-1$$

basterà calcolare il discriminante

$$\Delta=(\eta_0-\eta_1)^2$$

Ora abbiamo

$$\eta_0-\eta_1=\sum\varepsilon^a-\sum\varepsilon^b,$$

percorrendo a i residui quadratici e b i non residui (mod p); possiamo dunque scrivere

$$\eta_0-\eta_1=\sum_\mu(-1)^{\text{ind}\,\mu}\varepsilon^\mu,$$

percorrendo μ un sistema completo di resti (mod p), escluso lo zero. Ne deduciamo

$$(\eta_0-\eta_1)^2=\sum_\nu\sum_\mu(-1)^{\text{ind}\,\mu+\text{ind}\,\nu}\varepsilon^{\mu+\nu}$$

Eseguendo prima la sommazione rispetto a μ, possiamo cambiarvi μ in $\mu\nu$, giacché, restando fisso $\nu\neq 0$ (mod p),

$\mu\nu$ percorre insieme con μ un sistema completo di resti;
dunque

$$\Delta = \sum_{\nu} \sum_{\mu} (-1)^{\mathrm{ind}\,\mu} \varepsilon^{\nu(\mu+1)},$$

ovvero

$$\Delta = \sum_{\mu=1}^{\mu=p-1} (-1)^{\mathrm{ind}\,\mu} \left\{ \varepsilon^{\mu+1} + \varepsilon^{2(\mu+1)} + \cdots + \varepsilon^{(p-1)(\mu+1)} \right\}$$

la somma fra parentesi $\{\ \}$ è uguale a $p-1$ se $\mu+1 \equiv 0 \pmod p$ ed è $= -1$ in tutti gli altri casi, onde

$$\Delta = (-1)^{\mathrm{ind}\,(p-1)} \cdot p - \sum_{\mu=1}^{\mu=p-1} (-1)^{\mathrm{ind}\,\mu},$$

cioè

$$\Delta = (-1)^{\frac{p-1}{2}} \cdot p$$

essendo ora $(\eta_0 + \eta_1)^2 = 1$ avremo

$$\eta_0 \eta_1 = \frac{1 - (-1)^{\frac{p-1}{2}} \cdot p}{4}$$

e però la risolvente di 2° grado è la seguente

$$\eta^2 + \eta + \frac{1 - (-1)^{\frac{p-1}{2}}}{4} = 0$$

ed ha per radici

$$\eta_0 = \frac{-1 + \sqrt{(-1)^{\frac{p-1}{2}} \cdot p}}{2}, \quad \eta_1 = \frac{-1 - \sqrt{(-1)^{\frac{p-1}{2}} \cdot p}}{4}.$$

Dai teoremi generali risulta quindi:

L'equazione $x^{p-1} + x^{p-2} + \cdots + x + 1 = 0$ irriducibile nel campo assoluto di razionalità di venta riducibile appena aggiunta la irrazionalità $\sqrt{(-1)^{\frac{p-1}{2}} \cdot p}$, e si spezzerà in due fattori irriducibili di grado

$\frac{p-1}{2}$ (*)
I coefficienti di questi fattori saranno funzioni lineari intere a coefficienti interi di η_0, η_1 e però essi avranno la forma

$$\frac{y(x)+Z(x)\sqrt{(-1)^{\frac{p-1}{2}}\cdot p}}{2}$$

$$\frac{y'(x)-Z(x)\sqrt{(-1)^{\frac{p-1}{2}}\cdot p}}{2},$$

dove $y(x)$, $Z(x)$ sono polinomii a coefficienti interi. Ne risulta la formola notevole

$$4\,\frac{x^p-1}{x-1} = y^2(x) - (-1)^{\frac{p-1}{2}}\, p\, Z^2(x).$$

(*) La stessa cosa segue anche calcolando il discriminante D della equazione x^{p-1} che è dato dal determinante

$$D = \begin{vmatrix} s_0 & s_1 & s_2 & \cdots & s_{p-1} \\ s_1 & s_2 & s_3 & \cdots & s_p \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ s_{p-1} & s_p & s_{p+1} & \cdots & s_{2p-1} \end{vmatrix}$$

dove s_n indica la somma delle potenze n^{me} delle radici.
Ora si ha: $s_n = 0$ per $n \not\equiv 0 \pmod p$

$$s_p = p,$$

onde $$D = (-1)^{\frac{p-1}{2}} \cdot p^p.$$

Ora ogni irrazionale $\sqrt{D} = p^{\frac{p-1}{2}}\sqrt{(-1)^{\frac{p-1}{2}}\,p}$, il gruppo della proposta si riduce al sottogruppo d'indice 2 delle sostituzioni pari.

§. 93. — Teorema di reciprocità nella teoria dei residui quadratici

Dalla formola

$$(\eta_0 - \eta_1)^2 = (-1)^{\frac{p-1}{2}} \cdot p$$

che abbiamo sopra stabilita si può dedurre un' elegante dimostrazione della legge di reciprocità nella teoria dei residui quadratici; è questa la sesta dimostrazione di Gauss. Posto

$$S = \eta_0 - \eta_1 = \sum_{r=1}^{r=p-1} \left(\frac{r}{p}\right) \varepsilon^r,$$

essendo $\left(\frac{r}{p}\right)$ il noto simbolo di Legendre, cioè $\left(\frac{r}{p}\right) = \pm 1$ secondo che r è residuo o non residuo (mod p), avremo

$$S^2 = (-1)^{\frac{p-1}{2}} \cdot p.$$

Sia ora q un altro numero primo dispari; elevando ambo st'ultima formola alla potenza $\frac{q-1}{2}$ indi moltiplicando per S, abbiamo

$$S^q = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} p^{\frac{q-1}{2}} \cdot S,$$

da cui

$$(a) \qquad S^q - \left(\frac{q}{p}\right) S = \left\{(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right)\right\} S.$$

Ora

$$\left(\frac{q}{p}\right) S = \sum_{r=1}^{r=p-1} \left(\frac{qr}{p}\right) \varepsilon^r$$

e poichè qr percorre un sistema completo di resti (mod p), potremo cangiare sotto il segno Σ r in qr, il che dà

$$\left(\frac{q}{p}\right) S = \sum_{r=1}^{r=p-1} \left(\frac{r}{p}\right) \varepsilon^{qr}$$

La formola (a) si può anche scrivere

$$\left[\sum \left(\frac{r}{p}\right) \varepsilon^{r}\right]^q - \sum \left(\frac{r}{p}\right) \varepsilon^{qr} = \left\{(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right)\right\} \sum \left(\frac{r}{p}\right) \varepsilon^{r}$$

e riducendo gli esponenti di ε nel primo membro ai loro minimi resti (mod p), dovranno resultare i coefficienti uguali a quelli corrispondenti nel secondo (§. 87). Ora essendo

$$\left(\frac{r}{p}\right)^q = \left(\frac{r}{p}\right),$$

le potenze q^{me} dei termini della somma $\sum \left(\frac{r}{p}\right) \varepsilon^{r}$ si distinguono coi termini della seconda e risultanto gli altri coefficienti divisibili per q, avremo

$$(-1)^{\frac{p-1}{2}} q^{\frac{q-1}{2}} p^{\frac{q-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod q$$

ma, poichè

$$p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod q,$$

ne dedurremo

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}};$$

formola che esprime appunto la legge di reciprocità.

§. 94. — Applicazione delle formole di risoluzione delle equazioni Abeliane alle equazioni per la divisio

ne Del circolo. Abbiamo già detto, al §. 88, che la risolvente $F_e(\eta) = 0$ si risolve con l'estrazione d'un radicale d'indice e $\sqrt[e]{B}$ che porta sopra una quantità B razionalmente composta col la radice primitiva α d'ordine e dell'unità. Ci proponiamo ora di costruire effettivamente la quantità B, ciò che conduce a conseguenze aritmetiche di molto interesse. Faremo dapprima il calcolo sulla equazione stessa proposta

$$(1) \quad x^{p-1} + x^{p-2} + \ldots\ldots\ldots + x + 1 = 0$$

corrispondente al caso $e = p-1$; i risultati ottenuti daranno subito anche quelli relativi alla risolvente $F_e(\eta) = 0$. Secondo il metodo generale (§. 71) per la risoluzione delle equazioni Abeliane indichiamo con

$$x_0 = \varepsilon, x_1 = \varepsilon^g, x_2 = \varepsilon^{g^2} \ldots\ldots x_{p-2} = \varepsilon^{g^{p-2}}$$

le radici della (1), distribuite in un unico periodo, e con ω una radice primitiva della equazione $x^{p-1} = 1$, dobbiamo a quest'oggetto costruire la funzione razionale delle radici:

$$\varepsilon + \omega^h \varepsilon^g + \omega^{hb} \varepsilon^{g^2} + \ldots\ldots + \omega^{(p-2)b} \varepsilon^{g^{p-2}}$$

che indicheremo come al §. 71, col simbolo

$$(2) \quad (\omega^h, \varepsilon) = \sum_{\lambda=0}^{\lambda=p-2} \omega^{b\lambda} \varepsilon^{g^\lambda}.$$

In generale la (ω^h, ε) sarà razionalmente esprimibile per la (ω, ε) e la $(p-1)^{ma}$ potenza di questa sarà razional

mente noto nel campo ampliato coll'aggiunta di $\underline{\omega}$; indi per calcolare $\underline{\varepsilon}$ avremo la formola

$$(3) \qquad \varepsilon = \frac{1}{p-1}\left\{(1,\varepsilon)+(\omega,\varepsilon)+(\omega^2,\varepsilon)+\cdots\cdots+(\omega^{p-2},\varepsilon)\right\}$$

Dalla (2) si forma poi subito la corrispondente espressione risolvente per la $F_e(\eta)=0$; basta porvi per ciò

$$h = rf \quad (r=0,1,2\cdots\cdots e-1),$$

con che si ottiene

$$(\omega^{rf},\varepsilon) = \eta_0+\omega^{rf}\eta_1+\omega^{2rf}\eta_2+\cdots\cdots+\omega^{(e-1)rf}\eta_{e-1},$$

ossia poichè $\omega^f=\alpha$ è una radice primitiva della $x^e=1$, l'espressione

$$(4) \qquad (\alpha^r,\eta_0) = \eta_0+\alpha^r\eta_1+\alpha^{2r}\eta_2+\cdots\cdots\cdots+\alpha^{(e-1)r}\eta_{e-1}$$

formata nel modo del §. 71 colle radici di $F_e(\eta)=0$ e colle radici $\underline{\alpha}$ d'ordine $\underline{\varepsilon}$ della unità.

Ora si tratta di esprimere effettivamente

$$(\omega^h,\varepsilon) \text{ per } h=2,3,\cdots\cdots p-2$$

per (ω,ε) e la potenza $(\omega,\varepsilon)^{p-1}$ per ω, come analogamente $(\alpha^r\eta_0)$ per (α,η_0) e la potenza $(\alpha,\eta_0)^e$ per α.

§. 95. — Formole fondamentali per le espressioni (ω^h,ε).

Prendendo la radice primitiva g (mod p) per base di un sistema d'indici, la (2) si può

scrivere (*)
$$(\omega^h, \varepsilon) = \sum_{\mu=1}^{\mu=p-1} \omega^{h \operatorname{ind} \mu} \varepsilon^{\mu}.$$
Cangiando in questa ε in ε^{ν}, essendo $\nu \not\equiv 0 \pmod p$ abbiamo
$$(\omega^h, \varepsilon^{\nu}) = \sum_{\mu=1}^{\mu=p-1} \omega^{h \operatorname{ind} \mu} \varepsilon^{\mu\nu}$$
e poichè $\mu\nu$ percorre insieme con μ un sistema completo di resti $\pmod p$, possiamo anche scrivere
$$(H^*) \qquad (\omega^h, \varepsilon^{\nu}) = \omega^{-h \operatorname{ind} \nu} \sum_{\mu=1}^{\mu=p-1} \omega^{h \operatorname{ind} \mu} \varepsilon^{\mu}$$
il che dà la formola fondamentale
$$(5) \qquad (\omega^h, \varepsilon^{\nu}) = \omega^{-h \operatorname{ind} \nu} (\omega^h, \varepsilon).$$
Ora prendiamo due espressioni
$$(\omega^h, \varepsilon), \ (\omega^k, \varepsilon)$$
e moltiplichiamole fra loro; avremo
$$(\omega^h, \varepsilon)(\omega^k, \varepsilon) = \sum_{\mu} \sum_{\nu} \omega^{h \operatorname{ind} \mu + k \operatorname{ind} \nu} \varepsilon^{\mu+\nu},$$
facendo sì che μ e ν un sistema completo di resti $\pmod p$, escluso lo zero. Nella sommazione rispetto a ν, restando fisso μ, cangiamo ν in $\mu\nu$ ed otteniamo
$$(\omega^h, \varepsilon)(\omega^k, \varepsilon) = \sum_{\mu} \sum_{\nu} \omega^{(h+k) \operatorname{ind} \mu + k \operatorname{ind} \nu} \varepsilon^{\mu(\nu+1)}$$
che possiamo scrivere, invertendo le sommazioni
$$(6) \qquad (\omega^h, \varepsilon)(\omega^k, \varepsilon) = \sum_{\nu=1}^{\nu=p-1} \omega^{k \operatorname{ind} \nu} \sum_{\mu=1}^{\mu=p-1} \omega^{(h+k) \operatorname{ind} \mu} \varepsilon^{\mu(\nu+1)}$$

(*) In tutti i calcoli seguenti si tenga presente che l'uguaglianza $\varepsilon^r = \varepsilon^s$ avviene allorchè si abbia $r \equiv s \pmod p$ e l'altra $\omega^h = \omega^k$ allorchè sia invece $h \equiv k \pmod{p-1}$.

Ora distinguiamo due casi secondochè

$$h+k \not\equiv 0 \pmod{p-1}$$

ovvero

$$h+k \equiv 0 \pmod{p-1}.$$

1°. caso. Se $h+k \not\equiv 0 \pmod{p-1}$, la sommazione ridotta per i valori μ

$$\nu = 1, 2, 3, \ldots, p-2$$

dà per la (4^*) e la (5):

$$\sum_{\mu=1}^{\mu=p-1} \omega^{(h+k)\,ind\,\mu}\,\varepsilon^{\mu-(\nu+1)} = (\omega^{h+k}, \varepsilon^{\nu+1}) = \omega^{-(h+k)\,ind\,(\nu+1)}\,(\omega^{h+k}, \varepsilon),$$

mentre per $\nu = p-1$ si ha

$$\sum_{\mu=1}^{\mu=p-1} \omega^{(h+k)\,ind\,\mu} = 0$$

onde la (6) diventa

$$(\omega^h, \varepsilon)(\omega^k, \varepsilon) = (\omega^{h+k}, \varepsilon) \sum_{\nu=1}^{\nu=p-1} \omega^{k\,ind\,\nu - (h+k)\,ind\,(\nu+1)}$$

Si ha dunque la formula

$$(7)\quad (h+k \not\equiv 0 \pmod{p-1}) \qquad \frac{(\omega^h, \varepsilon)\,(\omega^k, \varepsilon)}{(\omega^{h+k}, \varepsilon)} = \sum_{\nu=1}^{\nu=p-2} \omega^{k\,ind\,\nu - (h+k)\,ind\,(\nu+1)}$$

che in ragione della simmetria del primo membro rispetto ad h ed k può anche scriversi

$$(7^*) \qquad \frac{(\omega^h, \varepsilon)(\omega^k, \varepsilon)}{(\omega^{h+k}, \varepsilon)} = \sum_{\nu=1}^{\nu=p-2} \omega^{h\,ind\,\nu - (h+k)\,ind\,(\nu+1)}$$

Il secondo membro della (7) o (7^*) è evidentemente della forma

$$\alpha_0 + \alpha_1 \omega + \alpha_2 \omega^2 + \cdots + \alpha_{p-2} \omega^{p-2}$$

essendo le α numeri razionali interi esso dicesi un numero **algebrico intero** nel campo $(1, \omega)$.

2°. caso. Sia ora $h+k \equiv 0 \pmod{p-1}$ allora la (6) diventa

$$(\omega^b, \varepsilon)(\omega^{-b}, \varepsilon) = \sum_{\nu=1}^{\nu=p-1} \omega^{-b \operatorname{ind} \nu} \sum_{\mu=1}^{\mu=p-1} \varepsilon^{\mu(\nu+1)}$$

Ora si ha

$$\varepsilon^{\nu+1} + \varepsilon^{2(\nu+1)} + \cdots\cdots + \varepsilon^{(p-1)(\nu+1)} = -1, \text{ per } \nu = 1, 2, 3 \cdots p-2$$

e invece $\varepsilon^{\nu+1} + \varepsilon^{2(\nu+1)} + \cdots\cdots + \varepsilon^{(p-1)(\nu+1)} = p-1$, per $\nu = p-1$,

onde $(\omega^b, \varepsilon)(\omega^{-b}, \varepsilon) = p\,\omega^{-b(\operatorname{ind}(p-1))} - \sum_{\nu=1}^{\nu=p-1} \omega^{-b \operatorname{ind} \nu}$

Ma si ha $\operatorname{ind}(p-1) = \frac{p-1}{2}$ e se $b \not\equiv 0 \pmod{p-1}$

è $\sum_{\nu=1}^{\nu=p-1} \omega^{-b \operatorname{ind} \nu} = 0$,

e però sussiste la formola

$$(8) \qquad (\omega^b, \varepsilon)(\omega^{-b}, \varepsilon) = (-1)^b p \qquad \left(b \not\equiv 0 \pmod{p-1}\right),$$

che è quella da sostituirsi alla (7) per $b + k \equiv 0 \pmod{p-1}$. Questa ci dimostra intanto che **nessuna delle espressioni (ω^b, ε) si annulla** ciò che è ben necessario osservare perchè i metodi generali per la risoluzione dell'equazione (Cfr. §. 72) riescano applicabili sotto la forma che qui consideriamo.

§. 76. — **Formole di risoluzione per l'equazione $F_\varepsilon(\eta) = 0$.** — Le formole fondamentali (7), (8) che abbiamo stabilite, conducono facilmente a risolvere la questione proposta. Se facciamo nella (7) $k = n\,b$, essendo n un intero, e supponiamo che dei tre numeri

$$(A) \qquad 2, \; n\,b, \; (n+1)\,b$$

non ve ne sia alcuno divisibile per $p-1$, otterremo

$$(9) \qquad (\omega^b, \varepsilon)\,(\omega^{nb}, \varepsilon) = (\omega^{(n+1)b}, \varepsilon)\,\psi_n(\omega^b),$$

ove si ponga per brevità

$$(10) \qquad \psi_n(\omega^b) = \sum_{\mu=1}^{\mu=p-2} (\omega^b)^{\mathrm{ind}\,\mu - (n+1)\,\mathrm{ind}\,(\mu+1)}$$

Questa quantità $\psi_n(\omega^b)$ viene quindi ad essere un numero complesso intero nel campo $(1, \omega^b)$. Supposto ora che fra i numeri

$$(B) \qquad b, 2b, 3b, \ldots\ldots mb$$

non ve ne sia alcuno divisibile per $p-1$, potremo fare successivamente nella (9)

$$n = 1, 2, 3 \ldots\ldots m-1$$

e moltiplicando tutte queste formole fra loro col togliere i fattori (non nulli) comuni alle due parti, risulterà:

$$(11) \qquad (\omega^b, \varepsilon)^m = (\omega^{mb}, \varepsilon)\,\psi_1(\omega^b)\,\psi_2(\omega^b) \ldots\ldots \psi_{m-1}(\omega^b).$$

Prendendo $m = 1$, possiamo prendere

$$m = 1, 2, 3 \ldots\ldots p-2$$

Poichè nessun numero della serie (B) sia divisibile per $p-1$ la (11) diventa

$$(12) \qquad (\omega, \varepsilon)^m = (\omega^m, \varepsilon)\,\psi_1(\omega)\,\psi_2(\omega) \ldots\ldots \psi_{m-1}(\omega),$$

Da questa formola caviamo

$$(\omega^2, \varepsilon), (\omega^3, \varepsilon) \ldots\ldots (\omega^{p-2}, \varepsilon)$$

e (ω, ε) come si voleva. Per esprimere la $(p-1)^{ma}$ radice di (ω, ε) razionalmente per ω, osserviamo che dalla (12) per

$m = p-2$ segue

$$(\omega, \varepsilon)^{p-2} = (\omega^{p-2}, \varepsilon)\psi_1(\omega)\psi_2(\omega)\cdots\cdots\psi_{p-3}(\omega)$$

e dalla (8) per $h=1$ $\quad (\omega, \varepsilon)(\omega^{p-2}, \varepsilon) = -p$

sicchè moltiplicando queste formole fra loro resulta la formola finale cercata

$$(13) \qquad (\omega, \varepsilon)^{p-1} = -p\,\psi_1(\omega)\,\psi_2(\omega)\cdots\cdots\psi_{p-3}(\omega).$$

Per ottenere le formole relative alla risolvente $F_2(\eta)=0$ facciamo nella (11) $h=f$ inoltre $\omega^h = \alpha$ e purchè si prenda $\underline{m}$ nella serie $\qquad 1, 2, 3, \cdots\cdots\cdots e-1,$

la serie (B) non conterrà numeri divisibili per $\underline{p-1}$ e la (11) diverrà $\quad (14) \quad (\alpha, \eta_0)^m = (\alpha^m, \eta_0)\,\psi_1(\alpha)\,\psi_2(\alpha)\cdots\cdots\psi_{m-1}(\alpha)$

indicando $\psi_n(\alpha)$ un numero complesso intero nel campo $(1, \alpha)$ dato dalla formola

$$(15) \qquad \psi_n(\alpha) = \sum_{\mu=1}^{\mu=p-2} \alpha^{\operatorname{ind}\mu - (n+1)\operatorname{ind}(\mu+1)}$$

Se osserviamo poi che in (8) per $h=f$ dà

$$(\alpha, \eta_0)(\alpha^{-1}, \eta_0) = (-1)^f p$$

e la (14) per $m = e-1$ diventa

$$(\alpha, \eta_0)^{e-1} = (\alpha^{-1}, \eta_0)\,\psi_1(\alpha)\,\psi_2(\alpha)\cdots\cdots\psi_{e-2}(\alpha);$$

moltiplicando le due ultime fra loro otteniamo

$$(16) \quad (\alpha, \eta_0)^e = (-1)^f p\,\psi_1(\alpha)\,\psi_2(\alpha)\cdots\cdots\psi_{e-2}(\alpha).$$

Questo e la (14) risolvono evidentemente per la $F_2(\eta)=0$ la questione proposta.

§. 97. — Numeri complessi $\psi_n(\alpha)$. Le formole di risoluzione per l'equazione

$$x^{p-1} + x^{p-2} + \cdots\cdots + x + 1 = 0$$

e per la risolvente $F_e(\eta) = 0$ si compongono, come si è visto, coi numeri complessi $\psi_n(\omega)$ e $\psi_n(\alpha)$ nei campi $(1, \omega)$, $(1, \alpha)$. Ci attieniamoci alquanto sul modo come questi numeri sono formati. Nella formola (15) che li definisce, essendo α una radice primitiva della $x^p = 1$, sostituiamo ad ogni esponente

$$\operatorname{ind} \mu - (n+1) \operatorname{ind} (\mu + 1)$$

il suo minimo resto positivo (mod e), che è un numero della serie

$$0, 1, 2 \cdots\cdots e-1,$$

e se indichiamo con A_ν il numero dei valori di μ per cui

$$\operatorname{ind} \mu - (n+1) \operatorname{ind} (\mu + 1) = \nu,$$

mentre μ prende i valori $1, 2, 3 \cdots\cdots p-2$, avremo evidentemente

$$(17) \qquad \psi_n(\alpha) = A_0 + A_1 \alpha + A_2 \alpha^2 + \cdots\cdots + A_{e-1} \alpha^{e-1}$$

e sarà

$$(18) \qquad A_0 + A_1 + A_2 + \cdots\cdots + A_{e-1} = p - 2.$$

Come esempio, consideriamo il caso

$$p = 29 \qquad e = \frac{p}{1}$$

e formiamo il numero

$$\psi_1(\alpha) \sum_{\mu=1}^{\mu=27} \alpha^{\operatorname{ind} \mu - 2 \operatorname{ind} (\mu+1)}$$

Serviamoci della seguente tavola di indici costruita colla radice primitiva $g = 2$.—

numero	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
indice	0	1	5	2	22	6	12	3	10	23	25	7	18	13	24	4	21	11	9	24	17	26	20	8	16	19	15	14

troviamo $A_0 = 4$ $A_1 = 4$ $A_2 = 0$ $A_3 = 4$ $A_4 = 6$ $A_5 = 3$ $A_6 = 6$,

cioè $\psi_1(\alpha) = 4 + 4\alpha + 4\alpha^3 + 6\alpha^4 + 3\alpha^5 + 6\alpha^6$

e anche essendo $\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha = -1$

$$\psi_1(\alpha) = 2\alpha^6 - \alpha^5 + 2\alpha^4 - 4\alpha^2.$$

Tratti i numeri complessi della forma

$$a_1\alpha + a_2\alpha^2 + \cdots + a_{e-1}\alpha^{e-1}$$

composti come i numeri $\psi_n(\alpha)$, in modo razionale intero con coefficienti interi per α dicansi **numeri interi del campo** $(1, \alpha)$. Come i numeri interi ordinari essi godono della proprietà di riprodursi per addizione (sottrazione) e moltiplicazione. Anche in questo campo di numeri si può stabilire il concetto della **divisibilità**, le cui leggi fondamentali valgono qui ancora(*). Tutti i numeri interi $\psi(\alpha)$

(*) 1°. Se due numeri sono divisibili per un terzo, tale è anche la loro somma o differenza.

2°. Se un numero a è divisibile per b e b per c sarà a divisibile per c.

del campo $(1, \alpha)$ che dividono 1 tali cioè che si abbia

$$1 = \varphi(\alpha)\, \psi(\alpha)$$

essendo $\psi(\alpha)$ un intero in $(1, \alpha)$ diconsi **unità** del campo $(1, \alpha)$. E mentre nel campo assoluto vi sono due sole unità $+1, -1$ qui invece abbiamo sempre innumerevoli unità eccettuati i casi $e = \bar{3}$, $e = 4$ (*), qui numero intero a del campo $(1, \alpha)$ è naturalmente divisibile per tutte le unità e se è divisibile soltanto per sè stesso e per le unità dicesi **indecomponibile** nel campo. Ma un numero indecomponibile nel campo $(1, \alpha)$ non ha più le proprietà essenziali dei numeri indecomponibili (primi) nel campo assoluto in particolare quello fondamentale di non poter dividere un prodotto se non divide uno dei fattori. Non è qui il luogo di spiegare come Kummer, colla sua creazione dei numeri ideali, è riuscito a ristabilire perfettamente in questa teoria le leggi dell'ordinaria divisibilità e come questi concetti siano stati poi portati da Dedekind al loro massimo grado di generalità nella teoria generale dei numeri algebrici (**)

(*) Nel caso $e = 3$ si hanno le 3 unità $1, \alpha, \alpha^2$ e per $e = 4$ le 4 unità $\pm 1, \pm i$.

(**) Veggasi l'appendice di **Dedekind** alle Vorlesungen.

§. 92. — Decomponibilità dei numeri primi $p \equiv 1 \pmod{e}$ nel campo $(1, \alpha)$.

Qui ci contenteremo di dimostrare come le formole sviluppate nei §. §. precedenti per la risoluzione della equazione $F_e(\eta) = 0$ permettano di effettuare una decomposizione di ogni numero $p \equiv 1 \pmod{e}$ nel campo $(1, \alpha)$.

Perciò supposto che fra i tre numeri

$$h, \; k, \; h+k$$

non ve ne sia alcuno divisibile per $p-1$, avremo dalla (7) §. 95

$$\frac{(\omega^h, \varepsilon)(\omega^k, \varepsilon)}{(\omega^{h+k}, \varepsilon)} = \sum_{\mu=1}^{\mu=p-2} \omega^{h \operatorname{ind} \mu - (h+k) \operatorname{ind}(\mu+1)}$$

ed anche

$$\frac{(\omega^{-h}, \varepsilon)(\omega^{-k}, \varepsilon)}{(\omega^{-(h+k)}, \varepsilon)} = \sum_{\mu=1}^{\mu=p-2} \omega^{-h \operatorname{ind} \mu + (h+k) \operatorname{ind}(\mu+1)}$$

e moltiplicando queste due formole fra loro coll'osservare che per la (8) si ha

$$(\omega^h, \varepsilon)(\omega^{-h}, \varepsilon) = (-1)^h p, \quad (\omega^k, \varepsilon)(\omega^{-k}, \varepsilon) = (-1)^k p$$
$$(\omega^{h+k}, \varepsilon)(\omega^{-(h+k)}, \varepsilon) = (-1)^{h+k} p,$$

otteniamo

$$p = \sum_{\mu=1}^{\mu=p-2} \omega^{h \operatorname{ind} \mu - (h+k) \operatorname{ind}(\mu+1)} \sum_{\mu=1}^{\mu=p-2} \omega^{-h \operatorname{ind} \mu + (h+k) \operatorname{ind}(\mu+1)}$$

Über Zahlen theorie di Dirichlet e Weber Algebra T II pag. 489 s. s.

E facendo ora come è lecito

$$h = f \qquad k = (e-2) f$$

indi $\omega^f = \alpha$, avremo la formola

$$(19) \qquad p = \sum_{\mu=1}^{\mu=p-2} \alpha^{\operatorname{ind}\mu + \operatorname{ind}(\mu+1)} \sum_{\mu=1}^{\mu=p-2} \alpha^{-\operatorname{ind}\mu - \operatorname{ind}(\mu a)}$$

che ci dà la decomposizione richiesta di p in due numeri **coniugati** del campo $(1, \alpha)$, dove è da osservarsi che questi numeri non sono unità, perchè se tale fosse l'uno lo sarebbe anche l'altro, mentre il loro prodotto p non è certamente un'unità.

Applichiamo da ultimo la decomposizione (19) ad un caso speciale facendo $e = 4$,

indi $\alpha = \sqrt{-1} = i$

e la (19) ci darà

$$p = \sum_{\mu=1}^{\mu=p-2} i^{\operatorname{ind}\mu + \operatorname{ind}(\mu+1)} \sum_{\mu=1}^{\mu=p-2} i^{\operatorname{ind}\mu - \operatorname{ind}(\mu a)}$$

Se indichiamo la prima somma con $a + ib$ essendo a, b numeri ordinari interi, avremo

$$p = (a+bi)(a-bi) = a^2 + b^2,$$

il che dà il teorema di Fermat:

Ogni numero primo della forma $4n+1$ è la somma di due quadrati.

§. 99. – Equazioni con un parametro.

Nelle equazioni a cui abbiamo applicato fin qui le teorie di Galois i coefficienti erano costanti assolute. Importa ora che ci occupiamo anche del caso in cui i coefficienti della proposta contengono un parametro arbitrario. Le più importanti equazioni che ci fornisce l'analisi, come le equazioni per la divisione dell'argomento nelle funzioni circolari o da ellittiche, e equazioni che si presentano nella teoria delle funzioni modulari ecc. appartengono appunto a questa categoria.

Indichiamo con x l'incognita nella nostra equazione e con t il parametro che supponiamo entrare razionalmente nei coefficienti; l'equazione si potrà scrivere

$$(1) \qquad f(x, t) = 0,$$

ove f è il simbolo di una funzione **razionale intera** in x, t. Ordiniamo f per le potenze di x e supponiamo che la (1) sia di grado m in x avremo:

$$(1^x) \qquad u_0 x^m + u_1 x^{m-1} + u_2 x^{m-2} + \cdots\cdots + u_{m-1} x + u_m = 0,$$

ove le u sono polinomii razionali interi in t. Ad ogni valore reale o complesso di t corrispondono in generale m valori finiti per x e cioè le radici

$$(2) \qquad x_1, x_2 \cdots\cdots x_m$$

della (1^x). Però quei valori speciali di t che annullano u_0 danno

no luogo ad una o più radici infinite nella serie (2)(*). Se si vuole evitare che per valori finiti di t possa diventare infinita una delle radici, basta moltiplicare la (1*) per a_0^{m-1} e ponendo $y = a_0 x$, la nuova equazione in y avrà il primo coefficiente $=1$ e gli altri razionali interi in t.
Se si esamina il modo com- nei §.§. 59 - 61 siamo pervenuti al concetto del gruppo di Galois per un'equazione, si vede subito che quelle considerazioni fondamentali rimangono ancora applicabili al caso attuale quando sia fissato il campo di razionalità.

$$(3) \qquad (R, R', R'' \cdots\cdots)$$

al quale naturalmente debbono appartenere i coefficienti dei polinomii $a_0\, a_1 \cdots a_{m-1}$ e a questo si aggiunge il parametro o l'indeterminata t.
Il gruppo G di Galois nel campo (3), cui sia stata aggiunta l'indeterminata t, si dirà il **gruppo algebrico** della equazione (1*) nel campo $(R, R', \widetilde{R''} \cdots\cdots)$. Le sue proprietà fondamentali sono come ben sappiamo, le seguen

(*) Precisamente r radici diventano infinite per $t = t_0$ se questo valore di t annulla $a_0\, a_1 \cdots\cdots a_{r-1}$ ma non annullare a.

ti:

1°. Se una funzione razionale $\psi(x_1, x_2 \ldots\ldots x_m, t)$ delle m radici della (1) e del parametro t con coefficienti razionali nel campo (3), rimane invariata per tutte le sostituzioni di G, effettuate sulle x, essa è una funzione razionale di t con coefficienti razionali in (3).

2°. Inversamente se la funzione razionale con coefficienti razionali: $\psi(x_1, x_2 \ldots\ldots x_m, t)$ è una funzione razionale di t con coefficienti razionali in (3), essa rimane invariata per qualsiasi sostituzione delle x del gruppo algebrico G.

§. 100.— **Gruppo di monodromia e sue proprietà.** Per lo studio delle equazioni con un parametro ha la massima importanza il gruppo di monodromia della equazione che definiamo come segue nel modo seguente:

Diciamo gruppo di monodromia della equazione (1) il gruppo di Galois che l'equazione acquista, quando per campo di razionalità si assume

quello di tutte le quantità costanti e a questo si aggiunge il parametro t.

Le proprietà fondamentali del gruppo Γ di monodromia si deducono da quelle ora enunciate pel gruppo algebrico G, mettendo la condizione che le funzioni da considerarsi abbiano coefficienti razionali, ove effettivamente riguardiamo ogni quantità costante come razionalmente nota. Così abbiamo:

1°. Ogni funzione razionale delle radici della (1) e del parametro t, che rimanga invariata per tutte le sostituzioni del gruppo Γ di monodromia, è esprimibile come funzione razionale della sola t.

2°. Inversamente se una funzione razionale di $x_1, x_2, \ldots\ldots x_m$ e di t è razionalmente esprimibile per la sola t, essa resta invariata per qualunque sostituzione del gruppo Γ di monodromia.

Queste proprietà sono caratteristiche per le sostituzioni del gruppo di monodromia e cioè:

Se una sostituzione sulle x lascia invariata qualunque funzione razionale delle x e di t, che sia razionalmente esprimibile per t, essa appartiene al gruppo Γ di monodromia.

È bene evidente che il gruppo Γ sarà monodromia è in ogni caso un sottogruppo del gruppo algebrico G; ma noi vogliamo ora dimostrare una proprietà di grande importanza e cioè che per ridurre il gruppo algebrico al gruppo di monodromia non importa aggiungere il campo razionale o (R, R', R''.....) a quello di tutte le quantità costanti, ma basta l'aggiunta di una **unica irrazionalità numerica** θ radice di una equazione normale

$$\varphi(\theta) = 0$$

con coefficienti razionali in (R, R', R''.....) : che ha per conseguenza che: **Il gruppo Γ di monodromia è in ogni caso sottogruppo invariante del gruppo algebrico G.**

§. 101. – **Il gruppo di monodromia come sottogruppo invariante del gruppo algebrico.** Per dimostrare il teorema enunciato

prendiamo una funzione razionale

$$y = \Psi(x_1, x_2 \ldots\ldots x_m t)$$

con coefficienti razionali in $(R, R', R'' \ldots\ldots)$ che rimanga invariata per tutte e sole le sostituzioni del gruppo Γ di monodromia e con questo costruiamo la risolvente

$$(H) \qquad \Phi(y, t) = 0$$

della proposta (1). Essendo la y invariabile per le sostituzioni di Γ, sarà esprimibile razionalmente per t, poniamo

$$y = \theta(t).$$

Immaginiamo al posto dei coefficienti nella θ sostituite altrettante indeterminate $\beta_1, \beta_2 \ldots\ldots \beta_n$; e sostituito questo valore di y nella (H). Ridurendo intera l'equazione così ottenuta ed eguagliando a zero i coefficienti delle varie potenze di t, si avrà un certo numero di equazioni con coefficienti razionali per determinare $\beta_1, \beta_2 \ldots\ldots \beta_n$;

queste equazioni sono certamente compatibili per ipotesi ne possono essere insufficienti, che altrimenti la (H) sarebbe soddisfatta da infinite funzioni razionali di t ciò che è assurdo. Ciascuna β è dunque un irrazionale numerico e sia la β_i radice dell'equazione irriducibile.

$F_i(\beta) = 0$

con coefficienti razionali in $(R, R', R'', \ldots)$.
Consideriamo l'equazione che si ottiene facendo il prodotto dei primi membri delle F_i differenti avremo un'equazione a radici disuguali, alla cui risolvente di Galois è possibile costruire la risolvente di Galois e basterà conoscere una radice α in questa per conoscere anche tutte le β. L'aggiunta di α al campo di razionalità fa scendere il gruppo G dell'equazione almeno a Γ, perchè dopo l'aggiunta di α la y è razionalmente nota per Γ; d'altronde è impossibile che G scenda ad un sottogruppo di Γ, giacchè persino nel massimo campo di razionalità costituito da tutte le quantità costanti, il gruppo della equazione è Γ. Dal teorema del §. 75, essendo α radice di un'equazione normale, segue allora che Γ è sottogruppo invariante di G; dunque:

Il gruppo Γ di monodromia di un'equazione ad un parametro è sempre sottogruppo invariante del suo gruppo algebrico G; per ridurre G a Γ basta aggiungere al campo di razionalità una sola irrazionalità numerica α, radice di un'equazione normale.

Osserviamo che quando il gruppo Γ di monodromia è transitivo l'equazione proposta è **irriducibile** nel senso che è impossibile scindere $f(x,t)$ nel prodotto di due funzioni $\varphi(x,t)$ $\psi(x,t)$ delle variabili x, t con coefficienti qualsiasi. La transitività del gruppo algebrico assicura soltanto che una tale decomposizione è impossibile **quando si esiga che** $\varphi(x,t)$, $\psi(x,t)$ **abbiano coefficienti razionali**. Dicendo che l'equazione $f(x,t)=0$ è irriducibile, intendiamo senz'altro che il suo gruppo di monodromia sia transitivo. Ove s'interpretino x, t come coordinate cartesiane di un punto variabile in un piano, ciò significa adunque che la curva $f(x,t)=0$ non si scinderà in curve di grado minore.

§. 102. — **Funzioni algebriche e punti critici**. Per fissare il concetto e stabilire le proprietà del gruppo di monodromia ci siamo valsi, nei §§. precedenti, di considerazioni puramente algebriche. Ma per ben intendere la natura di questo gruppo è indispensabile valersi anche di considerazioni che appartengono alla **teoria delle funzioni**, ciò che faremo ora limitandoci a quelle nozioni fondamentali.

Le m radici $x_1, x_2, \ldots, x_m$ della equazione $f(x,t)=0$ hanno per ogni valore di t ciascuna un valore; esse sono funzioni della variabile complessa t. Se la proposta è irriducibile (gruppo di monodromia intransitivo) esse sono proprio e semplicemente **gli m rami di una medesima funzione analitica x di t, che dicesi una funzione algebrica di t.** In generale per un valore assegnato di t i valori degli m rami sono distinti; coincideranno invece due o più rami quando per la coppia considerata di valori di x, t si annulli non solo la funzione $f(x,t)$ ma anche la sua derivata parziale rispetto alla x: $\frac{\partial f(x,t)}{\partial x}$. Eliminando la x fra le due equazioni

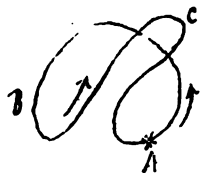
$$f(x,t)=0 \qquad \frac{\partial f(x,t)}{\partial x}=0,$$

si avrà un'equazione risultante in t (discriminante)

$$(5) \qquad F(t)=0,$$

le cui radici saranno tutti e soli quei valori di t per cui due di alcuni rami della funzione algebrica x vengono a coincidere. Immaginando i valori di t distesi sul piano complesso ovvero sulla sfera complessa, i punti di questo piano (in numero finito) che sono indici delle radici della (5) dicansi i punti **critici** della funzione algebrica x. Dimostriamo ora che l'indice di t tratto da un punto A del piano com-

plesso e descriva un cammino A C B che arrivi ad un'altro punto B senza passare per alcun punto critico. In ogni punto del cammino A C B gli n rami sono distinti e se partiamo da A scegliendo uno determinato fra gli n rami e durante il cammino A C B scegliamo sempre il valore per x che succede per continuità ai valori scelti nel cammino anteriore(*) arriveremo in B con un valore perfettamente determinato per x, che sarà uno degli n valori che la x ha in B. Pensiamo ora che si descriva un cammino chiuso A B C A il quale parta da A e vi ritorni, camminando intrecciandosi ma senza passare per alcun punto critico. Partendo da A con un determinato ramo x_1,



(*) Per fissare in modo più preciso, se con r indichiamo la minima distanza dei punti del cammino A C B dai vari punti critici, entro ogni cerchio di raggio r descritto col centro in un punto O della curva A C B, ciascuno delle funzioni $x_1, x_2, \ldots, x_n$ è finita continua e uniforme. Con un numero finito di tali cerchi, l'area di ciascuno dei essi avendo una parte comune con quella del successivo, è quindi possibile seguire in modo unico il prolungamento analitico, secondo Weierstrass, di uno qualcuno dei rami lungo A C B.

si ritorna in A avendo ancora uno degli m valori della x in A; che però potrà essere diverso da x_1, sia x_{i_1}. È chiaro che due rami diversi $x_1\ x_2$ saranno trasformati dopo descritto il cammino chiuso $ABCA$ in due rami diversi $x_{i_1}\ x_{i_2}$ perchè altrimenti, descrivendo il cammino in senso inverso, i due rami coincidenti $x_{i_1} = x_{i_2}$ sarebbero congiunti in rami diversi x_1, x_2, ciò che è assurdo. Così dunque l'effetto del cammino chiuso $ABCA$ sugli m rami

$$x_1\ x_2 \dots\dots x_m$$

sarà di congiungli negli m rami stessi

$$x_{i_1}\ x_{i_2} \dots\dots x_{i_m}$$

presi in un altro ordine, cioè: **Ogni cammino chiuso $ABCA$ produce sugli m rami una sostituzione**

$$S = \begin{pmatrix} x_{i_1} & x_{i_2} \dots\dots x_{i_m} \\ x_1 & x_2 \dots\dots x_m \end{pmatrix}$$

È chiaro che invertendo il senso percorrendo il cammino è inverso la sostituzione S si congiunge nella sua inversa S^{-1}. Se un terzo cammino chiuso C produce la sostituzione S e un secondo C' la sostituzione S', il cammino composto che risulta dal percorrere prima C poi C' (nel senso dovuto) produrrà precisamente la sostituzione prodotto SS'. Naturalmente la sostituzione S prodotta da un determinato cammino chiuso può anche essere l'identità 1. Si dimostra che ciò avviene certamente quando

il cammino chiuso sia tutto compreso in un'area priva di punti critici (*)

Ciò premesso se consideriamo tutti i possibili cammini chiusi che partano da A e vi ritornano otterremo un numero certamente finito di sostituzioni

$$S_1 \; S_2 \ldots\ldots S_n$$

sugli n rami. Vediamo subito che: Queste n sostituzioni formano un gruppo Λ. È invero se i cammini C_i, C_k producono le respettive sostituzioni S_i, S_k il cammino composto $C_i \; C_k$ produce come sopra si è detto, la sostituzione prodotto $S_i S_k$ che è dunque in Λ.

§. 103. — Nuova definizione del gruppo di monodromia. Ed ora è ben facile dimostrare: Il gruppo Λ delle sostituzioni $S_1, S_2 \ldots\ldots S_n$ che si producono sugli n rami per tutti i possibili

---

(*) Sussiste infatti il teorema che qui possiamo soltanto enunciare: In ogni area connessa del piano t priva di punti critici ciascuno degli n rami è una funzione continua e monodroma di t.

cammini chiusi, che partono da A e vi ritornano, coincide col gruppo Γ di monodromia.

In primo luogo vediamo subito che qualunque sostituzione S_i di Δ appartiene a Γ, per il che basta provare che S_i lascia invariata qualunque funzione razionale $\varphi(x, x_2, \dots x_m t)$ che sia razionale in t (§. 100). Ed invero se si ha

$$\varphi(x, x_2, \dots x_m t) = F(t),$$

essendo F razionale in t, per i principi della teoria delle funzioni, la relazione precedente rimarrà verificata lungo tutto il cammino chiuso che produce la S_i quindi anche al ritorno in A; se supponiamo ordinatamente

$$S_i = \begin{pmatrix} x_{i_1} & x_{i_2} & \dots & x_{i_m} \\ x_1 & x_2 & \dots & x_m \end{pmatrix}$$

ed osserviamo che $F(t)$, essendo razionale in t, al ritorno in A riprende il medesimo valore, avremo

$$\varphi(x_{i_1}, x_{i_2}, \dots x_{i_m} t) = \varphi(x_1, x_2, \dots x_m t) \text{ c. d. d.}$$

Per dimostrare inversamente che ogni sostituzione di Γ appartiene a Δ, come è necessario per potere affermare la coincidenza dei due gruppi, dobbiamo ricorrere al seguente teorema della teoria delle funzioni

Una funzione algebrica di una varia-

bile complessa t che sia monodroma in $\underline{t}$ è una funzione razionale di $\underline{t}$.

Ciò ammesso prendiamo una funzione razionale

$$\Psi = \Psi(x_1, x_2, \ldots, x_n, t)$$

invariabile per tutte e sole le sostituzioni di Λ, essa è certamente funzione algebrica di $\underline{t}$ come radice di una risolvente

$$\Phi(\Psi, t) = 0,$$

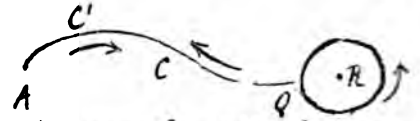
ma poichè per ogni cammino chiuso che da A ritorni in A, ove Ψ riprende il medesimo valore essa è razionale in $\underline{t}$ e perciò invariabile per tutte le sostituzioni del gruppo di monodromia Γ, il quale coincide adunque con Λ c. d. d.

È chiaro poi che mentre la definizione primitiva del gruppo Λ era relativa ad un punto A (non critico) fissato nel piano, risulta ora che questo gruppo Λ non varia se si cangia A, ciò che è facile vedere direttamente(*).

§. 10 H. — Punti di diramazione e sostitu

(*) Se si vuol trasportare A in A' basta sostituire ad ogni cammino chiuso γ per A un cammino equivalente (proveniente da la medesima sostituzione) che passa per A'. Basterà perciò aggiungere a C un cammino chiuso per A che passi per

zioni elementari del gruppo di monodromia. Risulta dai teoremi citati al §. 102 che se un cammino chiuso C si può per deformazione continua, senza mai attraversare punti critici, ridurre ad un altro cammino chiuso C', i due cammini C, C' produrranno sui rami la medesima sostituzione. Ora se Q è un punto critico, diremo **contorno elementare** o **ciclo** relativo al punto Q un cammino chiuso foggiato nel modo seguente. Descriviamo col centro in Q un cerchio di raggio piccolissimo, così che tutti gli altri punti critici rimangono esterni al cerchio $\underline{c}$, indi dal punto fissato A andiamo per un cammino rettilineo o curvilineo A C Q', ma che non passi per alcun punto critico, ad un punto Q' della circonferenza $\underline{c}$, descriviamo poi a partire da Q' (nel senso positivo) l'intiera circonferenza e ritorniamo da Q' in A pel medesimo cammino Q' C C'A. Il cammino chiuso così descritto sarà il ciclo relativo al punto Q. In generale questo ciclo produrrà un effettivo sostituzione sui rami (diversa dall'identica) e allora il punto Q si dirà un **punto di diramazione** della



A' senza includere punti critici.

funzione algebrica. Ma può anche darsi che la sostituzione si riduca all'identità, nel qual caso il punto Q si dirà un punto critico apparente.

Qualsiasi cammino chiuso può ridursi per deformazione continua ad una serie di cappii attorno agli effettivi punti di diramazione. Se supponiamo adunque che si abbiano r punti di diramazione

$$Q_1\ Q_2 \cdots\cdots Q_r$$

e i cappii corrispondenti producano le sostituzioni

$$s_1\ s_2 \cdots\cdots s_r,$$

ogni sostituzione S del gruppo di monodromia si potrà comporre per mezzo di queste r che sono adunque le sostituzioni generatrici del gruppo di monodromia. Con ciò non escludiamo naturalmente che fra le r sostituzioni s_i ve ne possono anche essere delle superflue(*).

§. 105. — Funzioni algebriche i cui rami sono funzioni lineari l'uno del

(*) Ciò avviene anzi necessariamente se fra i punti di diramazione $Q_1\ Q_2 \cdots\cdots Q_r$ includiamo quello che eventualmente si può avere in $t = \infty$.

l'altro. Un gruppo nettamente definito di equazioni con un parametro è quello di cui ora ci andiamo ad occupare, ricercando quelle funzioni algebriche per le quali tutti i rami sono funzioni lineari (fratte) a coefficienti costanti di uno qualunque dei rami stessi, il primo e più semplice esempio di tali equazioni ci è fornito dalla equazione ciclica $x^m = v$,
ove appunto tutti i rami si esprimono linearmente per uno x_0 colla formola

$$x_r = \varepsilon^r x_0 \qquad \begin{cases} \varepsilon = e^{\frac{2\pi i}{m}} \\ r = 1, 2, \cdots\cdots m-1. \end{cases}$$

Andiamo subito a dimostrare come il problema di costruire tutte le equazioni con un parametro, dotate della voluta proprietà, si riduca al problema già risoluto negli ultimi §§ della parte 1ª, alla determinazione dei gruppi finiti di sostituzioni lineari sopra una variabile x.

Sia $\qquad (1) \qquad f(x, t) = 0$

un'equazione irriducibile di grado m in x, tale che indicando con x un ramo qualunque, tutti gli altri rami siano funzioni lineari di x che indicheremo con

$$\frac{a_i x + b_i}{c_i x + a_i} \qquad (i = 1, 2 \cdots\cdots m-1)$$

le a, b, c, d essendo costanti. Se conveniamo di fare

$$a_0 = d_0 = 1 \quad , \quad b_0 = c_0 = 0,$$

potremo dire che tutti gli m rami della funzione algebrica $x(t)$ sono contenuti nella formula

$$(2) \qquad \frac{a_i x + b_i}{c_i x + d_i} \quad (i = 0, 1, 2 \ldots\ldots m-1).$$

Queste m sostituzioni lineari sulla variabile x formano un gruppo. Infatti consideriamo due qualunque dei rami

$$x' = \frac{a_i x + b_i}{c_i x + d_i} \quad , \quad x'' = \frac{a_k x + b_k}{c_i x + d_k} :$$

il gruppo Γ di monodromia, essendo transitivo, contiene certamente una sostituzione che trasporta il ramo x in $x' = \frac{a_i x + b_i}{c_i x + d_i}$ e quindi x'' nel nuovo ramo

$$\frac{a_i x'' + b_i}{c_i x'' + d_i} = \frac{a_i \dfrac{a_k x + b_k}{c_k x + d_k} + b_i}{c_i \dfrac{a_k x + b_k}{c_k x + d_k} + d_i}$$

Si ha dunque

$$\begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix} \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} = \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix}$$

essendo j uno degli m indici $0, 1, 2 \ldots\ldots m-1$. (*)

(*) In altre parole l'equazione

$$f\left(\frac{a_i x + b_i}{c_i x + a_i}, t\right) = 0$$

ammettendo la radice x dell'equazione irriducibile (1) le ammette

così vediamo che ad ogni equazione (1) della specie considerata corrisponde un gruppo finito (2) di sostituzioni lineari so= pra una variabile x.

§. 106. — **Costruzione delle equazioni dei poliedri regolari.** Inversamente dimostriamo che per ogni tale gruppo (2) si può costruire una corrispondente equazione (1). Prendiamo per ciò due costanti qualsiansi A, B colla sola condizione che esse non siano fra loro equivalenti rispetto al gruppo (2), cioè che non si abbia per alcun valore dell'indice i

$$B = \frac{a_i A + b_i}{c_i A + d_i},$$

e costruiamo la funzione razionale $f(x)$ data da

$$(3) \qquad f(x) = \frac{\prod_{i=0}^{i=m-1} \left(\frac{a_i x + b_i}{c_i x + d_i} - A \right)}{\prod_{i=0}^{i=m-1} \left(\frac{a_i x + b_i}{c_i x + d_i} - B \right)},$$

cioè

$$f(x) = \frac{\varphi(x)}{\psi(x)},$$

essendo $\varphi(x)$, $\psi(x)$ i due polinomii interi di grado m in x definiti dalle formole

---

mette inoltre, quindi anche $\frac{a_k x + b_k}{c_k x + d_k}$.

$$(4)\quad \begin{cases} \varphi(x) = \prod_{i=0}^{i=m-1} \{(a_i x + b_i) - A(c_i x + d_i)\} \\ \psi(x) = \prod_{i=0}^{i=m-1} \{(a_i x + b_i) - B(c_i x + d_i)\} \end{cases}$$

Per le ipotesi fatte si vede subito che i due polinomii $\varphi(x)$, $\psi(x)$ non hanno fattori comuni poichè le radici di $\varphi(x) = 0$ sono tutte in punti equivalenti al modo $x = \alpha$ a quelle di $\psi(x)$ similmente nei punti equivalenti a $x = \beta$. La funzione razionale $\mathfrak{F}(x) = \frac{\varphi(x)}{\psi(x)}$ gode evidentemente della proprietà di restare invariata per tutte le sostituzioni lineari sulla x appartenenti al gruppo (2).

Se si pone quindi, indicando con t un parametro,

$$\mathfrak{F}(x) = \frac{\varphi(x)}{\psi(x)} = t,$$

i vari rami della funzione algebrica x di t così definita dall'equazione irriducibile(*) (5) $\varphi(x) - t\,\psi(x) = 0$ saranno appunto legati ad uno di essi dalle sostituzioni lineari del gruppo (2).

Corrispondentemente ai cinque tipi di gruppi di sostituzioni

---

*) Che sia irriducibile risulta subito da ciò che ove $\varphi(x) - t\,\psi(x)$ si potesse scindere in due fattori l'uno di essi dovrebbe contenere linearmente e l'altro esserne indipendente, onde $\varphi(x)$, $\psi(x)$ avrebbero un fattore comune.

lineari avremo cinque tipi diversi di equazioni (5); queste diconsi le **equazioni dei poliedri regolari** perchè i gruppi corrispondenti dipendono appunto, nel modo che già abbiamo studiato, dai poliedri regolari.

§. 107. — **Gruppo di monodromia delle equazioni dei poliedri regolari.** È facile determinare il gruppo di monodromia della nostra equazione (5). Indicando infatti con

$$x_0\, x_1\, x_2 \cdots\cdots x_{m-1}$$

gli m rami ed applicandovi simultaneamente una sostituzione $\frac{a_i x + b_i}{c_i x + d_i}$ del gruppo (2), si produrrà sugli m rami una corrispondente sostituzione S_i. Le m sostituzioni

$$S_0 = 1,\ S_1,\ S_2 \cdots\cdots S_{m-1}$$

formano un gruppo Γ oloedricamente isomorfo col gruppo (2); questo gruppo Γ è precisamente il gruppo di monodromia della equazione (5). È infatti se prendiamo una funzione razionale

$$\Phi(x_0, x_1, x_2 \cdots\cdots x_{m-1}, t)$$

degli m rami e di t che rimanga invariata per tutte le sostituzioni S_i di Γ ed osserviamo che $x_1\, x_2 \cdots\cdots x_{m-1}$ sono funzioni lineari di x_0 potremo scrivere

$$\Phi(x_0\, x_1\, x_2 \cdots\cdots x_{m-1}\, t) = F(x_0, t),$$

essendo F razionale in x_0, t. In questa identità cangiando x_0 in x_i, si effettua sopra $x_0\, x_1 \cdots\cdots x_{m-1}$ una sostituzione di Γ e si ha perciò

$$F(x_0, t) = F(x_1, t) = \cdots = F(x_{m-1}, t),$$

onde $\Phi(x_0\, x_1 \cdots\cdots x_{m-1}\, t) = \frac{1}{m}\{F(x_0, t) + F(x_1, t) + \cdots + F(x_{m-1}, t)\}$ sarà razionalmente esprimibile per t. Il gruppo di monodromia della (5) coincide dunque con Γ o ne è un sottogruppo; ma quest'ultimo caso si esclude subito osservando che il gruppo di monodromia deve essere transitivo, a causa alle irriducibilità della (5), mentre Γ ha già il minimo ordine compatibile colla transitività. È chiaro poi che le quantità ora aggiungersi al campo di razionalità per risolvere il gruppo algebrico G al gruppo di monodromia Γ sono quelle che comparissono nei coefficienti a, b, c, d delle sostituzioni lineari del gruppo (2).

Quali saranno i punti critici della nostra equazione (5)? Per vederlo basta osservare che se per $t = t_0$ coincidono in x_0 p. es. ν rami, supponiamo

$$x_0\, x_1 \cdots\cdots x_{\nu-1},$$

tutti gli m rami coincideranno ν a ν e i corrispondenti $\frac{m}{\nu}$ valori distinti dei rami saranno precisamente i poli

(§. 113) delle sostituzioni del gruppo(*). Sono dunque tanti i punti critici della nostra equazione (5) quante classi di poli non equivalenti hanno le sostituzioni del gruppo e però secondo l'enumerazione dei possibili tipi del §. 114, avremo in ogni caso **tre punti critici** salvo per le equazioni appartenenti al tipo I (equazioni cicliche) ove il numero dei punti critici sarà di due soltanto.

§. 108. — **Sostituzioni omogenee del gruppo icosaedrale.** Le equazioni dei poliedri regolari appartenenti ai primi quattro tipi e cioè l'equazione della piramide e della doppia piramide regolare e quelle del tetraedro e dell'ottaedro hanno gruppi risolubili, esse sono quindi risolubili per radicali, cioè riducibili a successive equazioni binomie. Non così l'equazione dell'icosaedro il cui gruppo è semplice; l'irrazionalità semplice da essa definita (irrazionalità dell'icosaedro) è quindi di natura diversa da quelle definite per estrazioni di radicali.

(*) Si osservi che se i nomi $x_0\ x_1 \dots x_{\nu-1}$ coincidono ed $\begin{pmatrix} a, & b \\ c, & d \end{pmatrix}$ è una sostituzione del gruppo coincidono anche i ν nomi.

$$\frac{a x_0 + b}{c x_0 + d},\ \frac{a x_1 + b}{c x_1 + d} \dots\dots \frac{a x_{\nu-1} + b}{c x_{\nu-1} + d}$$

Se oltre all'aggiunta di radicali permettiamo quella di questa nuova irrazionalità, viene naturalmente ad ampliarsi il campo delle equazioni risolubili; in questo senso appunto, come vedremo, l'equazione generale di 5° grado diventa risolubile col nuovo mezzo. Ci proponiamo ora di studiare l'equazione dell'icosaedro e le sue più semplici risolventi per poi conoscere i principi della teoria di Klein dal cui libro (*) togliamo appunto, salvo piccole modificazioni, i §.§ seguenti.

I calcoli che dovremo eseguire verranno molto facilitati dall'uso delle variabili omogenee, applicando i primi teoremi della teoria delle forme, e perciò andiamo in primo luogo a scrivere sotto forma omogenea le sostituzioni del gruppo dell'icosaedro.

Osserviamo dapprima che se nella formola di Cayley (§.50)

$$(1)\quad z' = \frac{Az+B}{Bz+A_0}, \quad AA_0+BB_0=1$$

congiungiamo la variabile z nel quoziente di due nuove variabili $\frac{z_1}{z_2}$ e similmente la trasformata z' in $\frac{z_1'}{z_2'}$, alla sostituzio

---

(*) Klein — Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade (Leipzig Teubner 1884).

ne non omogenea (1) possiamo coordinare l'altra omogenea

$$(2)\quad \begin{cases} \pm z'_1 = A z_1 + B z_2 \\ \pm z'_2 = -B_0 z_1 + A_0 z_2 \end{cases}$$

nella quale fissando che il determinante debba essere l'unità resterà ancora da scelta fra i due segni. Per ciò ad ogni sostituzione non omogenea (1) ne corrisponderanno due omogenee (2), ed una di queste una sola delle (1). Se consideriamo un gruppo G_N di N sostituzioni (1) avremo corrispondentemente un gruppo G_{2N} di $2N$ sostituzioni (2), che è evidentemente isomorfo col grado 2 di meriedria con G_N, all'identità in G_N corrispondendo in G_{2N} il sottogruppo invariante d'ordine 2 formato dall'identità e dalla sostituzione $z'_1 = -z_1, \quad z'_2 = -z_2$.

Qui si presenta naturalmente la domanda (*) È possibile fra le due determinazioni di segno nella (2) sceglierne una in guisa da ottenere un gruppo omogeneo di N sostituzioni oloedricamente isomorfo con G_N? A noi ci basta osservare che ciò è già impossibile per un gruppo diedrale di H sostituzioni (Vierergruppe).

(*) Klein-Thomaeder pag. 45.

è infatti a queste quattro sostituzioni rossiamo dare la forma normale (§. 45)

$$z' = \pm z_1 \qquad z' = \pm \frac{1}{z} i$$

le corrispondenti 8 sostituzioni omogenee sono

$$\begin{pmatrix} \pm 1, & 0 \\ 0, & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm i, & 0 \\ 0, & \mp i \end{pmatrix}, \begin{pmatrix} 0, & \pm i \\ \pm i, & 0 \end{pmatrix}, \begin{pmatrix} 0, & \pm 1 \\ \mp 1, & 0 \end{pmatrix}$$

e il quadrato di $\begin{pmatrix} \pm i, & 0 \\ 0, & \mp i \end{pmatrix}$ dà la sostituzione $\begin{pmatrix} -1, & 0 \\ 0, & -1 \end{pmatrix}$ che figura dunque necessariamente nel gruppo. Ora il gruppo dell'icosaedro (come pure quello del tetraedro e dell'ottaedro) contiene dei gruppi dicerali di 4 sostituzioni e però anche qui la cosa domandata è impossibile.

Per scrivere le sostituzioni omogenee del gruppo dell'icosaedro basterà prendere questo gruppo sotto la forma normale della Parte 1ª §. 48, ricordando che le due sostituzioni elementari del gruppo icosaedrale sono le due seguenti

$$S) \; z' = \varepsilon z \qquad T) \; z' = \frac{(\varepsilon^4 - \varepsilon) z + (\varepsilon^2 - \varepsilon^3)}{(\varepsilon^2 - \varepsilon^3) z - (\varepsilon^4 - \varepsilon)}$$

e riducendo le corrispondenti omogenee ad determinante 1, avremo:

$$(6) \qquad \text{per la } S \begin{cases} z_1' = \pm \varepsilon^2 z_1 \\ z_2' = \mp \varepsilon^2 z_2 \end{cases}$$

$$(8^4) \qquad \text{per la } T \begin{cases} \sqrt{5}\, z_1' = \pm \{(\varepsilon^4 - \varepsilon) z_1 + (\varepsilon^2 - \varepsilon^3) z_2\} \\ \sqrt{5}\, z_2' = \pm \{(\varepsilon^2 - \varepsilon^3) z_1 - (\varepsilon^4 - \varepsilon) z_2\} \end{cases}$$

Queste sostituzioni omogenee formano l'intero gruppo ecc.

genere G_{120}. È bene osservare che siccome il gruppo icosaedrale G_{60} è semplice, il gruppo omogeneo $\bar{G}_{120}$ non ammette alcun altro sottogruppo invariante all'infuori del gruppo delle due sostituzioni

$$\begin{cases} z'_1 = z_1 \\ z'_2 = z_2 \end{cases} \qquad \begin{cases} z'_1 = -z_1 \\ z'_2 = -z_2 \end{cases}$$

§ 104. — **Forme invarianti del gruppo omogeneo icosaedrale. Una forma binaria $\Phi(z_1, z_2)$ si dirà un invariante del gruppo icosaedrale quando per ogni sostituzione del gruppo G_{120} essa si riproduca, a meno d'un fattore costante.**

Eguagliando a zero una tale forma $\Phi(z_1, z_2) = 0$, i valori radicii $z = \frac{z_1}{z_2}$ avranno per indici sulla sfera complessa un sistema di punti, che per ogni rotazione del gruppo icosaedrale ritornerà in sè stesso. Viceversa se si ha un tale sistema di punti e si costruisce la funzione $F(z)$ che li ha per indici delle sue radici e mutando z in $\frac{z_1}{z_2}$ col moltiplicare $F\left(\frac{z_1}{z_2}\right)$ per la conveniente potenza di z_2 si cangia $F\left(\frac{z_1}{z_2}\right)$ in una forma $\Phi(z_1, z_2)$ sarà evidentemente $\Phi(z_1, z_2)$ un invariante del gruppo icosaedrale. Un primo vantaggio della

introduzione delle variabili omogenee consiste in ciò che l'eventuale valore $z = \infty$ fra i punti radici viene caratterizzato dal presentarsi nella forma $\Phi(z, z_2)$ come fattore una certa potenza di z_2. Se il sistema dei punti radici della forma invariante $\Phi(z_1, z_2)$ si scinde in più sistemi di punti equivalenti rispetto al gruppo delle 60 rotazioni, la forma $\Phi(z, z_2)$ si scinderà nel prodotto di altrettante forme parziali che diremo **forme fondamentali**. In generale una forma fondamentale dell'icosaedro sarà di grado = 60, poichè ogni punto radice, per le 60 rotazioni dell'icosaedro, occupa 60 posizioni distinte. Fanno soltanto eccezione i 12 vertici dell'icosaedro, i 20 punti medii delle faccie (proiettati dal centro sulla sfera), e infine i 30 punti medi delle costole. Corrispondentemente avremo tre forme fondamentali dei gradi 12, 20 e 30 che indicheremo rispettivamente con

$$f, \quad H, \quad T$$

Se indichiamo con N il grado di una forma invariante qualsiasi dovremo quindi avere

$$(a) \qquad N = \alpha \cdot 60 + \beta \cdot 12 + \gamma \cdot 20 + \delta \cdot 30$$

essendo $\alpha, \beta, \gamma, \delta$ numeri interi positivi o nulli.

È facile vedere a priori che per ogni sostituzione omogenea di G_{120} ciascuna di queste tre forme si riproduce a meno

lutamente (è un invariante assoluto). E infatti poniamo che p. e. la f acquisti per le dette sostituzioni i fattori

$$(7) \qquad a, b, c \ldots\ldots;$$

siccome a f per le due sostituzioni s, s' acquista i rispettivi fattori α, α', per la sostituzione prodotta s s' acquista il fattore prodotto $\alpha\alpha'$, i numeri (7) dovranno formare un gruppo nel senso che il prodotto di due numeri nella serie (7) si troverà nella serie stessa. Se indichiamo con ν il numero dei fattori distinti (7) e con $\varepsilon = e^{2\pi\frac{i}{\nu}}$ una radice primitiva d'ordine ν dell'unità vediamo subito(*) che i fattori (7) sono in altro ordine le potenze di ε

$$1, \varepsilon, \varepsilon^2 \ldots\ldots \varepsilon^{\nu-1}.$$

Quelle sostituzioni di G_{120} che lasciano f assolutamente invariata formano un sottogruppo invariante in G_{120} d'indice $= \nu$ onde per l'osservazione in fine al §. precedente, sarà a $\nu = 1$ o $\nu = 60$ o $\nu = 120$. D'altra parte se $\nu > 1$, non può avere che uno dei tre

---

(*) Essendo ν l'ordine del gruppo (7) si ha

$$a^\nu = b^\nu = c^\nu = \ldots\ldots\ldots = 1$$

onde $a, b, c \ldots\ldots$ sono radici ν^{me} dell'unità e poichè sono in numero di ν distinte sono appunto potenze di una radice primitiva ε.

valori $\nu = 2, \quad \nu = 3, \quad \nu = 5$

che si presentano come periodi del gruppo icosaedrale di rotazioni, perchè se indichiamo con A una delle rotazioni cui corrisponde per la f la moltiplicazione per ε e con ν il periodo di A alla $A^\nu = 1$ (la f essendo di grado pari) corrisponderà certamente $\varepsilon^\nu = 1$ poichè la sostituzione omogenea corrispondente dovrà essere $z_1' = \pm z_1, \quad z_2' = \pm z_2$.

Ne concludiamo dunque $\nu = 1$ c. d. d.

Se consideriamo le potenze

$$f^5, \quad H^3, \quad T^2$$

avremo tre forme di grado 60 e con due qualunque di esse potremo comporre linearmente, con coefficienti costanti, qualsiasi forma fondamentale $\Phi(z_1, z_2)$ cioè sussisterà p. e. la formola (8) $\Phi = \lambda f^5 + \mu H^3$ (λ, μ costanti)

è infatti evidente che per qualunque valore del parametro $\lambda : \mu$ si ha nel secondo membro una forma invariante fondamentale dell'icosaedro; d'altronde dando a $\frac{\lambda}{\mu}$ un conveniente valore possiamo far coincidere una radice di $\frac{\lambda}{\mu} f^5 + H^3 = 0$ con una di Φ dopo di che coincideranno tutte le loro (60) radici e si avrà la (8).

In particolare resulta di qui che fra le tre potenze f^5, H^3, T^2 sussiste una relazione lineare omo-

genera a coefficienti costanti.

§. 110. — Costruzione delle forme icosaedrali f, H, T.

Cominciamo dal costruire la forma f, i cui punti radii sono nei 12 versi dell'icosaedro, cioè nei punti (§. 55)

$$z = \infty,\ \infty,\ \varepsilon^r(\varepsilon+\varepsilon^4),\ \varepsilon^r(\varepsilon^2+\varepsilon^3) \quad (r = 0, 1, 2, 3, 4)$$

Possiamo quindi porre

$$f = z_1 z_2 \prod_{r=0}^{r=4}\{z_1 - \varepsilon^r(\varepsilon+\varepsilon^4)z_2\}\prod_{r=0}^{r=4}\{z_1 - \varepsilon^r(\varepsilon^2+\varepsilon^3)z_2\}$$

e poichè si ha in generale

$$\prod_{r=0}^{r=4}(z_1 - \varepsilon^r z_2) = z_1^5 - z_2^5$$

sarà $f = z_1 z_2\{z_1^5 - (\varepsilon+\varepsilon^4)^5 z_2^5\}\{z_1^5 - (\varepsilon^2+\varepsilon^3)^5 z_2^5\}$

Ora, essendo $(\varepsilon+\varepsilon^4)(\varepsilon^2+\varepsilon^3) = -1$

$$(\varepsilon+\varepsilon^4)^5 + (\varepsilon^2+\varepsilon^3)^5 = -11,$$

troviamo

$$(9) \qquad f = z_1 z_2(z_1^{10} + 11 z_1^5 z_2^5 - z_2^{10}).$$

Per calcolare H e T potremmo similmente servirci dei valori di z nei loro punti radicii, ciò che otterremo cercando i poli delle rispettive rotazioni coi periodi 2 e 3. In modo più breve ed elegante troviamo le forme H e T osservando che la forma Hessiana della f, cioè il determinante

$$\begin{vmatrix} \frac{\partial^2 f}{\partial z_1^2} & \frac{\partial^2 f}{\partial z_1 \partial z_2} \\ \frac{\partial^2 f}{\partial z_2 \partial z_1} & \frac{\partial^2 f}{\partial z_2^2} \end{vmatrix}$$

è appunto di grado 20 ed essendo un covariante di f essa rimane, come f, totalmente invariata per ogni sostituzione omogenea del gruppo icosaedrale. Nella formola del §. precedente, essendo qui $N = 20$, si ha necessariamente

$$\alpha = \beta = \delta = 0 \quad , \quad \gamma = 1$$

cioè l'Hessiana di f a meno di un fattore numerico coincide con H. Poniamo con Klein

$$H = \frac{1}{11^2} \begin{vmatrix} \frac{\partial^2 f}{\partial x_1^2} & \frac{\partial^2 f}{\partial x_1 \partial x_2} \\ \frac{\partial^2 f}{\partial x_1 \partial x_2} & \frac{\partial^2 f}{\partial x_2^2} \end{vmatrix}$$

e col calcolo effettivo troviamo

$$(10) \quad H = -(x_1^{20} + x_2^{20}) + 228(x_1^{15} x_2^5 - x_1^5 x_2^{15}) - 494\, x_1^{10} x_2^{10}.$$

Similmente è un covariante di f il Jacobiano di f e di H

$$\begin{vmatrix} \frac{\partial f}{\partial x_1} & \frac{\partial H}{\partial x_1} \\ \frac{\partial f}{\partial x_2} & \frac{\partial H}{\partial x_2} \end{vmatrix}$$

e il suo grado essendo appunto = 30 si vede che esso, a meno di un fattore numerico è = T. Poniamo:

$$T = -\frac{1}{20} \begin{vmatrix} \frac{\partial f}{\partial x_1} & \frac{\partial f}{\partial x_2} \\ \frac{\partial H}{\partial x_1} & \frac{\partial H}{\partial x_2} \end{vmatrix}$$

e troviamo

$$(11) \quad T = x_1^{30} + x_2^{30} + 522(x_1^{25} x_2^5 - x_1^5 x_2^{25}) - 10005(x_1^{20} x_2^{10} + x_1^{10} x_2^{20})$$

come già abbiamo detto al §109, il quadrato della forma T è una combinazione lineare omogenea di f^5 e H^3:

$$T^2 = \lambda f^5 + \mu H^3$$

e basta confrontare i coefficienti di z_1^{60} e $z_1^{55} z_2^5$ da una parte e dall'altra per trovare

$$\mu = -1 \qquad \lambda = 1728 = 12^3$$

cioè come relazione fra f^5, H^3, e T^2:

$$(12) \qquad T^2 + H^3 = 1728 f^5$$

§. 111. — **L'equazione dell'icosaedro.** Per le osservazioni generali al §. 106 si ottiene l'equazione dell'icosaedro eguagliando il quoziente di due forme fondamentali di grado 60 ad un parametro $\underline{t}$, e ponendo $x = \frac{z_2}{z_1}$. Di quanto poi abbiamo detto alla fine del §. 109 risulta che l'arbitrarietà che resta nella costruzione della equazione stessa equivale al far subire al parametro $\underline{t}$ una sostituzione lineare fratta. Possiamo con Klein l'equazione dell'icosaedro ponendo

$$(13) \qquad \frac{H^3}{12^3 f^5} = Z$$

avendo qui indicato con z il parametro; per l'identità (12) potremo anche scrivere, sotto forma di proporzione continua:

$$(13^*) \qquad Z : Z-1 : 1 = H^3 : T^2 : 12^3 f^5$$

L'equazione del 60° grado dell'icosaedro scritta per disteso sarà dunque

$$(14) \qquad (x^{20} - 228 x^{15} + 494 x^{10} + 228 x^5 + 1)^3 - 12^3 Z x^5 (x^{20} + 11 x^5 - 1)^5 = 0.$$

essa definisce una funzione algebrica $\underline{X}$ di Z, i cui 60 rami si ottengono l'uno dall'altro colle 60 sostituzioni del gruppo icosaedrale. I tre punti critici dell'equazione (14) dell'icosaedro (§. 10 7) sono rispettivamente in

$$Z = 0, \quad Z = 1, \quad Z = \infty,$$

ai quali corrispondono per la $\underline{X}$ valori che sono gli indici dei punti medii delle facce, o dei punti medii delle costole e infine dei vertici stessi dell'icosaedro, come si vede dalla (13*). La nostra rappresentazione geometrica rende evidente che girando attorno al punto critico $Z = 0$ i 60 rami dell'icosaedro subiscono una sostituzione del 3° ordine (si permutano tre a tre), attorno al punto $Z = 1$ si permutano due a due e infine attorno al punto $Z = \infty$ ha luogo una permutazione dei rami cinque a cinque. Sappiamo già che il gruppo Γ di monodromia dell'equazione dell'icosaedro è precisamente d'ordine 60 ed effettivamente isomorfo col gruppo di rotazioni dell'icosaedro (§. 10 7): l'irrazionalità numerica la cui aggiunta abbassa il gruppo algebrico G al gruppo Γ di monodromia è qui precisamente la radice 5^{a} ε dell'unità che comparisce razionalmente nei coefficienti delle sostituzioni del gruppo icosaedrale. Quale sarà adunque il gruppo algebrico G dell'equazione (14) dell'icosaedro nel campo $\Omega(\varepsilon)$ di razionalità?

Siccome l'equazione

$$\varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0$$

che definisce l'irrazionalità ε ha un gruppo d'ordine $= 4$ (§. 86), in ordine al teorema generale del §. 20, G, che dovrà contenere Γ come sottogruppo invariante (§ 101), avrà un ordine m dato da $m = 4 \times 60$ ovvero $m = 2 \times 60$

Il secondo caso è da escludersi perchè coll'estrazione di una radice quadrata G si abbasserebbe a Γ e però il ramo εx_0 potendosi esprimere linearmente per x_0, dovrebbe essere nota ε, esattamente una sola radice quadrata, ciò che è assurdo.

§. 112. — **Metodo invariativo di Klein per la formazione delle risolventi.** L'equazione dell'icosaedro possiede diverse risolventi della cui formazione vogliamo ora occuparci. Ma qualunque di queste risolventi, il gruppo icosaedrale G_{60} essendo semplice, ha un gruppo oloedricamente isomorfo con G_{60}.

Queste risolventi corrispondono a diversi sottogruppi di G_{60} ed hanno gradi rispettivamente uguali agli indici dei sottogruppi. Ogni sottogruppo di G_{60}, essendo un gruppo di sostituzioni lineari sopra una variabile, rientrerà in uno dei [illegible] tipi fondamentali. È facile enumerare i

possibili sottogruppi, che saranno necessariamente ciclici o diedrali, o infine tetraedrali. Abbiamo così:

1) sottogruppi ciclici del 2° ordine
2) " ciclici del 3° ordine
3) " ciclici del 5° ordine
4) sottogruppi diedrali del 4° ordine
5) " diedrali del 6° ordine
6) " diedrali del 10° ordine
7) sottogruppi tetraedrali (del 12° ordine);

la loro effettiva esistenza risulta subito dalla ispezione diretta del gruppo icosaedrale (§. 54). Così i sottogruppi diedrali del 10° ordine sono quelli che lasciano fisso un diametro dell'icosaedro; essi sono tutti affini fra loro in numero di 6. I sottogruppi tetraedrali sono quelli che lasciano fermo uno dei cinque ottaedri che hanno per vertici i punti medii delle costole dell'icosaedro; abbiamo 5 tali sottogruppi affini fra loro. L'equazione dell'icosaedro possiede quindi risolventi dei rispettivi gradi

$$30, 20, 12, 15, 10, 6, 5.$$

Le ultime due corrispondenti ai sottogruppi diedrali G_{10} e ai sottogruppi tetraedrali G_{12}, hanno per noi uno speciale interesse e di queste esclusivamente ci occuperemo.

Per la formazione effettiva delle risolventi possiamo servirci dell'elegante metodo di Klein(*) che utilizza le proprietà invariative e che andiamo ora a descrivere riferendoci, per fissare le idee, alla risolvente di 5° grado. Scelto uno dei cinque sottogruppi tetraedrali, prendiamo una forma $\varphi_0(z, z_n)$ che rimanga invariata per tutte e sole le corrispondenti sostituzioni tetraedrali, dalla quale per le sostituzioni omogenee icosaedrali otteniamo cinque forme distinte

$$\varphi_0 \quad \varphi_1 \quad \varphi_2 \quad \varphi_3 \quad \varphi_4 ,$$

indi formiamo il prodotto

$$\prod_{n=0}^{n=4} (\varphi - \varphi_n),$$

essendo φ un'indeterminata. Nel corrispondente polinomio di 5° grado

$$\varphi^5 + a\varphi^4 + b\varphi^3 + c\varphi^2 + d\varphi + e$$

i coefficienti $a, b, \ldots\ldots$, come funzioni simmetriche elementari di $\varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4$, sono forme icosaedrali e perciò funzioni razionali intere di f, H, T che è facile determinare conoscendo i rispettivi gradi di $a, b, c \ldots\ldots$ e i loro coefficienti numerici. Così le 5 forme φ_n sono radici della equazione di 5° grado

$$(15) \qquad \varphi^5 + a\varphi^4 + b\varphi^3 + c\varphi^2 + d\varphi + e = 0$$

(*) Ikosaeder pag. 98.

i cui coefficienti sono razionali interi in f, H, T. Per cangiarla in una risolvente dell'equazione dell'icosaedro basta moltiplicare o dividere φ per tali potenze di f, H, T da ottenere una funzione omogenea di grado zero in z_1, z_2 cioè una funzione razionale di $x = \frac{z_1}{z_2}$.

§. 113. — **Le forme ottaedrali $\underline{t}$ e $\underline{W}$.** Per costruire una risolvente di 5° grado della equazione dell'icosaedro dobbiamo scegliere, per quanto sopra si è detto, una forma $\varphi(z_1, z_2)$ appartenente ad uno dei cinque sottogruppi tetraedrali, una tale forma è p.e. quella di 6° ordine le cui radici sono sei vertici di uno dei cinque ottaedri iscritti nell'icosaedro, Ne costruiamo una, che indicheremo con t, e quindi tutte le altre osservando che, secondo quanto è detto al §. 118, le tre sostituzioni

$$T \quad , \quad U \quad , \quad TU$$

insieme coll'identità formano il sottogruppo G_4 contenuto in uno dei cinque sottogruppi tetraedrali e i prodotti di queste tre sostituzioni sono appunto i sei vertici di uno degli ottaedri. Orbene per queste tre sostituzioni abbiamo la respettiva rappresentazione analitica (l. c)

$$T) \quad z' = \frac{(\varepsilon^3 - \varepsilon^4)z + (\varepsilon^2 - \varepsilon^3)}{(\varepsilon^3 - \varepsilon^2)z - (\varepsilon^4 - \varepsilon)}$$

$$U) \quad z' = -\frac{1}{z}$$

$$\text{TU)}\quad x' = \frac{(\varepsilon^2-\varepsilon^3)x+(\varepsilon-\varepsilon^4)}{(\varepsilon-\varepsilon^4)x-(\varepsilon^2-\varepsilon^3)}$$

e quindi le forme di 2° grado che hanno le radici nei loro fo. li sono(*)

$$\begin{cases} z_1^2 - 2(\varepsilon^2+\varepsilon^3)\, z_1 z_2 - z_2^2 \\ z_1^2 + z_2^2 \\ z_1^2 - 2(\varepsilon+\varepsilon^4)\, z_1 z_2 - z_2^2 \end{cases}$$

Possiamo prendere t semplicemente eguale al prodotto di queste tre forme: onde risulta

$$t = (z_1^2 + z_2^2)(z_1^4 + 2z_1^3 z_2 - 6z_1^2 z_2^2 - 2z_1 z_2^3 + z_2^4),$$

ovvero

$$(16)\quad t = z_1^6 + 2z_1^5 z_2 - 5z_1^4 z_2^2 - 5z_1^2 z_2^4 - 2z_1 z_2^5 + z_2^6.$$

Una seconda forma che rimane invariata per le sostituzioni dei vertici sottogruppo tetraedrale è quella che ha per radici gli otto punti medii delle facce dell'ottaedro considerato (proiettati dal centro sulla sfera). Mediante considerazioni perfettamente simili a quelle del §. 118, vediamo che una tale forma W è, a meno di un fattore numerico, la forma Hessiana di t, che è appunto di 8° grado. Poniamo

$$W = \frac{1}{5^2 \cdot 4^2} \begin{vmatrix} \frac{\partial^2 t}{\partial z_1^2} & \frac{\partial^2 t}{\partial z_1 \partial z_2} \\ \frac{\partial^2 t}{\partial z_1 \partial z_2} & \frac{\partial^2 t}{\partial z_2^2} \end{vmatrix}$$

e troveremo

$$(17)\quad W = -(z_1^8 + z_2^8) + 7(z_1^7 z_2 - z_1 z_2^7) - 7(z_1^6 z_2^2 + z_1^2 z_2^6) - 7(z_1^5 z_2^3 - z_1^3 z_2^5)$$

(*) Si abbia riguardo alle formole $\varepsilon^4 - \varepsilon = (\varepsilon^2-\varepsilon^3)(\varepsilon^2+\varepsilon^3)$, $\varepsilon^2 - \varepsilon^3 = (\varepsilon-\varepsilon^4)(\varepsilon+\varepsilon^4)$

Qualunque altra forma invariabile per le sostituzioni del sottogruppo tetraedrale in considerazione si esprimerà per le due fondamentali t e W (cf. §. 10°). Per le 60 rotazioni dell'icosaedro ovvero per le 120 sostituzioni del gruppo omografico icosaedrale(*), le nostre forme t, W si mutano rispettivamente in 5 forme distinte che otteniamo applicando le potenze S^ν della sostituzione fondamentale S cioè, sotto forma omogenea le sostituzioni

$$S^\nu) \quad x_1' = \mp \varepsilon^{3\nu} x_1, \quad x_2' = \pm \varepsilon^{2\nu} x_2 \quad \text{per } \nu = 0, 1, 2, 3, 4$$

Indicando i rispettivi valori di t, W con t_ν, W_ν avremo

$$(16^*) \quad t_\nu = \varepsilon^{3\nu} x_1^6 + 2\varepsilon^{\nu} x_1^3 x_2^3 - 5\varepsilon^{2\nu} x_1^4 x_2^2 - 5\varepsilon^{4\nu} x_1^2 x_2^4 - 2\varepsilon^{3\nu} x_1 x_2^5 + \varepsilon^{2\nu} x_2^6$$

$$(17^*) \quad W_\nu = -\varepsilon^{4\nu} x_1^8 + \varepsilon^{3\nu} x_1^7 x_2 - 7\varepsilon^{2\nu} x_1^6 x_2^2 - 7\varepsilon^{\nu} x_1^5 x_2^3 + 7\varepsilon^{4\nu} x_1^3 x_2^5 - 7\varepsilon^{3\nu} x_1^2 x_2^6 - \varepsilon^{2\nu} x_1 x_2^7 - \varepsilon^{\nu} x_2^8$$

Le 60 rotazioni dell'icosaedro permuteranno fra loro le cinque forme t_ν o le W_ν precisamente come i cinque ottaedri corrispondenti a cui ci riportiamo alla rappresentazione geometrica del §. 54 osservando che le denominazioni ivi date A, B, C, D, E pei cinque ottaedri corrispondono agli attuali indici 0, 1, 2, 3, 4 vediamo subito che la rotazione elementare S produce la sostituzione ciclica del 5° ordine

---

(*) Si consideri che la t, W, come forme di grado pari, restano invariate per la sostituzione $x_1' = -x_1$, $x_2' = -x_2$.

$$(t_0\ t_1\ t_2\ t_3\ t_4) \quad o \quad (W_0\ W_1\ W_2\ W_3\ W_4)$$

e la rotazione elementare T i rispettivi prodotti di due trasposizioni

$$(t_1\ t_2)(t_3\ t_4) \quad o \quad (W_1\ W_2)(W_3\ W_4),$$

restando fisso t_0 o W_0.

§. 114. — **Le risolventi di 5° grado delle $\underline{u}$ e delle $\underline{r}$.** Calcoliamo in primo luogo, secondo la (15) §. 113 l'equazione

$$t^5 + a t^4 + b t^3 + c t^2 + d t + e = 0$$

le cui radici sono t_0, t_1, t_2, t_3, t_4. I coefficienti

$$a, b, c, d, e$$

sono rispettivamente forme icosaedrali dei gradi

$$6, 12, 18, 24, 30$$

e però si ha:

$$a = 0, \quad b = kf, \quad c = 0, \quad d = lf^2, \quad e = mT,$$

essendo k, l, m costanti numeriche, sicchè l'equazione sarà

$$t^5 + kf \cdot t^3 + lf^2 \cdot t + mT = 0 \ldots$$

Per determinare i valori di k, l, m possiamo servirci delle formole di Newton, che danno qui:

$$kf = -\frac{1}{2}\Sigma t_r^2, \quad lf^2 = \frac{1}{2}k^2 f^2 - \frac{1}{4}\Sigma t_s^4$$

$$mT = -\Pi t_r$$

e paragonando nelle tre formole i coefficienti dei rispetti

vi termini di più alto grado

$$z_1^{11} z_{\infty 1}, \quad z_1^{22} z_{\infty 1}^2, \quad z_1^{30}$$

osservando le (16*), si trova

$$k = -10, \quad l = 45 \quad m = -1$$

onde per l'equazione richiesta

$$(18) \qquad t^5 - 10 f t^3 + 45 f^2 t - T = 0.$$

Per cangiare questa in una risolvente icosaedrale, secondo quanto si è detto alla fine del §. 112, basterà cangiare t, moltiplicando e dividendo per potenze di f, H, T, in una forma di grado zero in z_1, z_∞. Poniamo

$$u = \frac{12 f^2 t}{T}$$

con che appunto u resulterà funzione di $x = \frac{z_1}{z_\infty}$, e la (18) avendo riguardo all'equazione (13*) §. 111 dell'icosaedro, diventa:

$$(19) \qquad 11 u^5 (1 - Z)^2 - 10 u^3 (1 - Z) + 1 = 0$$

che è la risolvente di 5° grado della equazione dell'icosaedro, chiamata da Klein la risolvente delle u.

Una seconda risolvente, la risolvente delle v, si ottiene ponendo

$$v = \frac{t^2}{f}.$$

Per calcolarla scriviamo la (18) così:

$$T = t (t^4 - 10 f t^2 + 45 f^2);$$

quadrando e dividendo per f^5, col sostituire a $\frac{t^2}{f}$ la v, abbiamo:

$$(19^*) \qquad v (v^2 - 10 v + 45)^2 + 12^3 (Z - 1) = 0$$

e questa è la risolvente delle x.

Quale è il gruppo di queste risolventi? Quanto al gruppo di monodromia esso è il gruppo alterno G_{60} sulle cinque radici come risulta subito dai teoremi generali (cfr. §. 112). Il gruppo algebrico nel campo assoluto di razionalità sarà G_{60} stesso o il gruppo totale G_{120} sulle 5 radici. Per decidere la questione basta considerare la radice quadrata del discriminante della (19) o della (19*) che essendo invariabile per il gruppo di monodromia G_{60} sarà certo razionale in z e i coefficienti, se il gruppo algebrico è il gruppo totale, dovranno contenere come irrazionalità numerica una radice quadrata (di un numero intero). Ora se costruiamo la radice quadrata del discriminante della (18), cioè

$$\prod_{r<s} (t_r - t_s),$$

basterà osservarne un valore numerico speciale p. e. per $z_0 = 0 \quad z_1 = 1$. Siccome t_r diventa ε^{r^2}, questo valore numerico non differisce dalla radice quadrata del discriminante dell'equazione

$$x^4 + x^3 + x^2 + x + 1 = 0,$$

che contiene l'irrazionalità $\sqrt{5}$ (§ 92). Dunque:

Le risolventi di 5° grado (19) (19*) dell'icosaedro hanno nel campo assoluto di razionalità pa

gruppo algebrico il gruppo totale il quale viene abbassato al gruppo alterno, gruppo di una sostituzione, coll'aggiunta di $\sqrt{5}$.

§. 115. — La risolvente principale delle Y. Per la risoluzione della equazione generale di 5° grado mediante la irrazionalità icosaedrica hanno grande importanza quelle speciali risolventi di 5° grado dell'icosaedro in cui mancano la quarta e la terza potenza dell'incognita e di queste appunto vogliamo ora occuparci. Appartiene a questa specie l'equazione che ha per radici

$$W_0, W_1, W_2, W_3, W_4$$

giacchè ΣW_n e ΣW_n^2, non esistendo forme icosaedrali di 1° e 16° grado, sono identicamente nulle. Lo stesso dicasi dell'equazione che ha per prodotti

$$t_0 W_0, t_1 W_1, t_2 W_2, t_3 W_3, t_4 W_4$$

giacchè non esistono forme icosaedrali dei gradi 14 e 28. Ma si ha anche

$$\Sigma W_n . \Sigma t_n W_n = 0$$

giacchè il primo membro è una forma icosaedrale di grado 22 e però identicamente nulla. Ne deduciamo che ponendo (20) $Y_n = \sigma W_n + \tau t_n W_n$,

con σ, τ costanti anche l'equazione di 5° grado di cui sono radici $Y_0\ Y_1\ Y_2\ Y_3\ Y_4$ mancherà della 4^a e 3ª potenza. Volendo calcolare effettivamente la corrispondente equazione che scriveremo

$$Y^5 + 5\alpha\, Y^2 + 5\beta\, Y + f = 0$$

cominceremo dall'osservare che si ha

$$f = -\prod_{r=0}^{r=4}(\sigma W_r + \tau t_r W_r)$$

cioè

$$f = -\prod_{r=0}^{r=4}(W_r)\cdot\prod_{r=0}^{r=4}(\sigma + \tau t_r)$$

Ora $\Pi(W_r)$ è una forma icosaedrale di grado 10 e per la formola (a) §. 109 si vede che essa non può differire da H^2 che per un coefficiente numerico; troviamo quindi subito

$$\Pi(W_r) = -H^2$$

D'altronde dalla (18) §. 114, indicando con λ una arbitraria ricordiamo l'identità

$$\lambda^5 - 10 f \lambda^3 + 45 f^2 \lambda - T = \Pi(\lambda - t_r)$$

onde, facendo $\lambda = -\frac{\sigma}{\tau}$, resulta

$$\Pi(\sigma + \tau t_r) = \sigma^5 - 10 f \sigma^3 \tau^2 + 45 f^2 \sigma \tau^4 + T\tau^5$$

e perciò

$$f = H^2[\sigma^5 - 10 f \sigma^3 \tau^2 + 45 f^2 \sigma \tau^4 + T\tau^5]$$

Per calcolare poi α, β converrà nuovamente ricorrere alle formole di Newton che danno

$$-15\alpha = \Sigma(\sigma W_r + \tau t_r W_r)^3$$

$$-20\beta = \Sigma(\sigma W_r + \tau t_r W_r)^4$$

e si troverà così

$$\begin{cases} \alpha = \beta f^2 \sigma^3 + T\sigma^2\tau + \gamma = f^3\sigma\tau^2 + fT\tau^3 \\ \beta = -fH\sigma^4 + 18f^2H\sigma^2\tau^2 + HT\sigma\tau^3 + 27f^3H\tau^4. \end{cases}$$

Per cangiare nuovamente l'equazione di 5° grado nelle Y in una risolvente icosaedrale, poniamo come sopra

$$u = \frac{12f^2t}{T}$$

e inoltre $v = \frac{12fW}{H}$; allora la (20) si scrive

$$Y_2 = m v_2 + n u_2 v_2$$

ove si ponga

$$m = \frac{\sigma H}{12f}, \qquad n = \frac{\tau H T}{12^2 f^2}.$$

Sostituendo i valori che ne risultano per σ, τ nelle equazioni in Y, questa diventa:

$$(21)\quad Z y^5 + 5y^2\left(8m^3 + 12m^2n + \frac{6mn^2+n^3}{1-z}\right) + 15y\left(-4m^4 + \frac{6m^2n^2+4mn^3}{1-z} + \frac{3n^4}{4(1-z)^2}\right) +$$
$$+ 3\left(48m^5 - \frac{40m^3n^2}{1-z} + \frac{15mn^4+4n^5}{(1-z)^2}\right) = 0$$

Questa si dirà la risolvente principale di 5° grado dell'equazione dell'icosaedro. Manifestamente per la determinazione del suo gruppo valgono le considerazioni stesse della fine del §. precedente. Il suo gruppo algebrico nel campo assoluto di razionalità (aggiuntevi m, n e z) è il gruppo totale sulle 5 radici; esso si abbassa al gruppo alterno, che è il gruppo di monodromia, aggiungendo l'irrazionalità quadratica $\sqrt{5}$ (*)

(*) Per vedere ciò basta fare p. e. $m=1$, $n=0$ e considerare che il pro-

Le risolventi di 5° grado (19), (19*), (21) che noi abbiamo determinato sono tutte trasformate di Tschirnhaus l'una dell'altra ed è facile trovare ad esempio le formule che esprimono u e $\mathcal{T}$ razionalmente per $\underline{r}$ (V. Klein Ikosaeder pag. 106).

§. 116. — **La risolvente di 6° grado.** Occupiamoci ora di costruire una risolvente di 6° grado. Prendiamo perciò come forma di 4° grado che rimane invariata per un sottogruppo diedrale G_{10} semplicemente la seguente

$$\varphi = 5 z_1^2 z_2^2$$

che rimane invariata per il sottogruppo diedrale

$$G_{10} = (S^2, U S^2)$$

che lascia fisso il diametro congiungente i punti $z=0$, $z=\infty$(*). Applicando alla φ la sostituzione T, sotto la forma omogenea (6*) §. 108, ne otteniamo la nuova forma

$$\varphi_0 = (z_1^2 + z_1 z_2 - z_2^2)^2$$

che per la S^2 si cangia in generale in

---

dotto $\Pi(W_r - W_s)$ contiene appunto l'irrazionalità $\sqrt{5}$ giacchè p.e. se si fa $z_2 = 0$ $z_1 = 1$ diventa $W_r = -\varepsilon^{-r}$.

(*) Il prodotto semplice $z_1 z_2$ cangierebbe invece di segno per la sostituzione U, che scritta sotto forma omogenea è: $z_1' = \pm z_2$, $z_2' = \mp z_1$.

$$\varphi_r = (\varepsilon^r z_1^2 + z_1 z_2 - \varepsilon^{4r} z_2^2)^2$$

Contraddistinguendo il valore primitivo di φ coll' indice ∞:

$$\varphi_\infty = 5 z_1^2 z_2^2$$

costruiamo l' equazione di 6° grado

$$\varphi^6 + a'\varphi^5 + b'\varphi^4 + c'\varphi^3 + d'\varphi^2 + e'\varphi + f' = 0$$

che ha per radici

$$\varphi_\infty \ \varphi_0 \ \varphi_1 \ \varphi_2 \ \varphi_3 \ \varphi_4$$

I suoi coefficiente $a', b', \ldots\ldots$ saranno forme icosaedrali dei gradi $4, 8, 12, 16, 20, 24,$

e però avremo

$$a' = b' = d' = 0, \quad c' = hf, \quad e' = kH, \quad f' = lf^2$$

con h, k, l coefficienti numerici che si determinano nel solito metodo paragonando i termini corrispondenti. Troviamo così:

$$\varphi^6 - 10 f \varphi^3 + H\varphi + 5f^2 = 0$$

e per cangiare questa in una risolvente icosaedrale poniamo p. e.

$$\zeta = \frac{H\varphi}{12 f^2}$$

Sostituendo avremo

$$(22) \quad \zeta^6 - 10 Z \zeta^3 + 12 Z^2 \zeta + 5 Z^2 = 0.$$

Quale sarà il gruppo di risolvente di 6° grado? Il suo gruppo di monodromia è oloedricamente isomorfo col gruppo alterno su 5 lettere ed è quindi necessariamente il gruppo modulare (P.e 1a § ..) sulle 6 radici. Ciò si conferma di=

rettamente osservando che la rotazione S produce sulle φ la sostituzione ciclica

$$(\varphi_0\ \varphi_1\ \varphi_2\ \varphi_3\ \varphi_4)$$

lasciando ferma φ_∞ mentre la T dà

$$(\varphi_\infty\ \varphi_0)\ (\varphi_1\ \varphi_4)\ (\varphi_2\ \varphi_3),$$

cioè sugli indici abbiamo rispettivamente le sostituzioni

$$\nu' \equiv \nu + 1, \qquad \nu' \equiv -\frac{1}{\nu} \pmod 5$$

che sono appunto le sostituzioni elementari del gruppo modulare (§. 30). Quanto poi al gruppo algebrico osserviamo che dovendo contenere come sottogruppo invariante il gruppo modulare, o coinciderà con questo o sarà il gruppo lineare totale di 120 sostituzioni

$$\nu' \equiv \frac{\alpha\nu + \beta}{\gamma\nu + \delta} \pmod 5 \qquad \alpha\delta - \beta\gamma \not\equiv 0 \pmod 5$$

Per decidere quale dei due casi ha luogo si consideri la radice quadrata del discriminante dell'equazione in φ e facendo p. e. $z_2 = 0 \quad z_1 = 1$, con che

$$\varphi_\infty = 0 \qquad \varphi_2 = \varepsilon^{22},$$

si vedrà subito che esso contiene l'irrazionalità $\sqrt{5}$. Dunque: Il gruppo algebrico della risolvente di 6° grado (22) è il gruppo lineare totale; questo si abbassa al gruppo modulare, che è il gruppo di monodromia, aggiungendo l'irrazionalità quadratica

$\sqrt{5}$.

le circostanze qui notate non sono che casi particolari di quelle che si presentano nella teoria delle equazioni modulari ellittiche; ma noi non possiamo in questo luogo occuparci ulteriormente.

§. 117. — L'equazione generale principale di 5° grado e la sua risolvente di Galois icosaedrale. L'equazione principale di 5° grado (21) ammette come risolvente di Galois (dopo aggiunta l'irrazionalità $\sqrt{5}$ con che la radice quadrata del suo discriminante risulta razionalmente nota) precisamente l'equazione dell'icosaedro. Ora noi ci proponiamo di dimostrare che se si prende un'equazione **principale** di 5° grado qualunque cioè della forma

$$(23)\qquad y^5 + 5\alpha y^2 + 5\beta y + \gamma = 0,$$

essendo α, β, γ costanti qualsiasi e si aggiunga al campo di razionalità la radice quadrata del discriminante D, sarà possibile costruire una risolvente di Galois che sia precisamente una equazione icosaedrale. Si farà poi, come subito dimostreremo, si può ridurre coll'estrazione di una sola radice quadrata, l'equazione generale di 5° grado alla principale (23)

equazione generale di 5° grado si può risolvere coll'aggiunto di una irrazionalità icosaedrica ed estrazioni di radici quadrate.

Per dimostrare in primo luogo che l'equazione generale di 5° grado si può ridurre, estraendo una radice quadrata, alla forma principale (23) osserviamo che in generale che se

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots\dots + a_{n-1} x + a_n = 0$$

è un'equazione di grado n, di cui costruiamo una trasformata di Tschirnhaus colla funzione trasformatrice

$$y = d_1 + d_2 x + \dots\dots + d_n x^{n-1}$$

e indichiamo con

$$y^n + A_1 y^{n-1} + A_2 y^{n-2} + \dots\dots + A_n = 0$$

l'equazione trasformata, sarà in generale A_2 una forma di grado 2 nelle d con coefficienti razionalmente noti per le a. Possiamo quindi rendere $A_1 = 0$ e $A_2 = 0$, prendendo p. e.

$$y = d_1 + d_2 x + d_3 x^2$$

e risolvendo successivamente un'equazione di 1° grado. Così in particolare, per $n = 5$, riduremo l'equazione alla forma principale (23).

Ciò premesso, all'oggetto di costruire una risolvente icosaedrale alla (23), esaminiamo dapprima come per l'equazione principale (21) una tale risolvente icosaedrale è effettivamente

costruita, in qual modo cioè la radice $x=\frac{z_1}{z_2}$ dell'equazione dell'iperaereo si esprime razionalmente per le radici

$$y_0, y_1, y_2, y_3, y_4$$

della (21). Per ciò dalle formole (16*) (17*) §. 113 deduciamo

$$W_2=(\varepsilon^{42}z_1-\varepsilon^{32}z_2)(7z_1^2z_2^5-z_1^7)-(\varepsilon^{22}z_1+\varepsilon^2z_2)(z_2^7+7z_1^5z_2^2)$$

$$t_2W_2=(\varepsilon^{42}z_1-\varepsilon^{32}z_2)\ (26z_1^{10}z_2^3+39z_1^5z_2^8+z_2^{13})$$
$$(\varepsilon^{22}z_1+\varepsilon^2z_2)\ (z_1^{13}-39z_1^8z_2^5-26z_1^3z_2^{10})$$

onde segue che la y_2, data dalla (20) §. 115, assume la forma

$$y_2=(\varepsilon^{42}z_1-\varepsilon^{32}z_2)R+(\varepsilon^{22}z_1+\varepsilon^2z_2)S,$$

essendo R, S espressioni lineari in σ, τ. Ora costruiamo le due espressioni seguenti

$$y_0+\varepsilon y_1+\varepsilon^2y_2+\varepsilon^3y_3+\varepsilon^4y_4$$
$$y_0+\varepsilon^2y_1+\varepsilon^4y_2+\varepsilon y_3+\varepsilon^3y_4$$

e troveremo

$$y_0+\varepsilon y_1+\varepsilon^2y_2+\varepsilon^3y_3+\varepsilon^4y_4=5z_1R$$
$$y_0+\varepsilon^2y_1+\varepsilon^4y_2+\varepsilon y_3+\varepsilon^3y_4=-5z_2R$$

di cui la formola cercata

$$(24)\qquad x=\frac{z_1}{z_2}=-\frac{y_0+\varepsilon y_1+\varepsilon^2y_2+\varepsilon^3y_3+\varepsilon^4y_4}{y_0+\varepsilon^2y_1+\varepsilon^4y_2+\varepsilon y_3+\varepsilon^3y_4}$$

che esprime la radice $\underline{x}$ della risolvente iperaereale razionalmente per le radici dell'equazione principale di 5° grado (21).

Poichè, come si è visto al §. 113, alle rotazioni elementari S.T dell'icosaedro corrispondono rispettivamente le sostituzioni

$$(y_0\, y_1\, y_2\, y_3\, y_4)\ ,\ (y_1\, y_2)(y_3\, y_4)$$

sulle radici y_r, inversamente ne segue che se nella espressione (24) della x si eseguiscono queste permutazioni elementari del gruppo alterno sulle y, la x subirà le due sostituzioni elementari del gruppo icosaedrale

$$x' = \varepsilon x\,, \qquad x' = \frac{(\varepsilon^4-\varepsilon)x + (\varepsilon^2-\varepsilon^3)}{(\varepsilon^2-\varepsilon^3)x - (\varepsilon^4-\varepsilon)}$$

Notiamo subito che mentre la prima formola e cioè

$$\frac{y_1+\varepsilon y_2+\varepsilon^2 y_3+\varepsilon^3 y_4+\varepsilon^4 y_0}{y_1+\varepsilon^2 y_2+\varepsilon^4 y_3+\varepsilon y_4+\varepsilon_2 y_0} = \varepsilon\,\frac{y_0+\varepsilon y_1+\varepsilon^2 y_2+\varepsilon^3 y_3+\varepsilon^4 y_4}{y_0+\varepsilon^2 y_1+\varepsilon^4 y_2+\varepsilon y_3+\varepsilon^3 y_4}$$

sussisterebbe anche se le y fossero fra loro indipendenti, la seconda invece non è una identità nelle y e sussiste soltanto in forza delle relazioni

$$\sum y_r = 0 \qquad \sum y_r^2 = 0\,.$$

§. 118. — La radice λ della risolvente icosaedrale.

I risultati precedenti conducono naturalmente a ricercare se per una equazione principale di 5° grado qualsiasi (23) accade quello che abbiamo visto verificarsi per la (21) e cioè se ponendo

$$(25) \qquad \lambda = -\frac{y_0+\varepsilon y_1+\varepsilon^2 y_2+\varepsilon^3 y_3+\varepsilon^4 y_4}{y_0+\varepsilon^2 y_1+\varepsilon^4 y_2+\varepsilon y_3+\varepsilon^3 y_4}$$

ed eseguendo le permutazioni elementari del gruppo ottaedrico sulle radici y_r:

$$(y_0\, y_1\, y_2\, y_3\, y_4)\,,\quad (y_1\, y_2)(y_3\, y_4)\,,$$

la funzione razionale λ delle radici subirà le sostituzioni elementari

$$\lambda' = \varepsilon\lambda\,, \qquad \lambda' = \frac{(\varepsilon^4-\varepsilon)\lambda + (\varepsilon^4-\varepsilon^3)}{(\varepsilon^2-\varepsilon^3)\lambda - (\varepsilon^4-\varepsilon)}$$

del gruppo icosaedrale il che appunto vogliamo ora constatare. Quanto alla prima sostituzione, come già sopra si è notato, la verifica è immediata. Per la seconda riesce più complicata la cosa, dovendosi tener conto delle relazioni

$$(26) \qquad \sum y_r = 0 \qquad \sum y_r^2 = 0\,,$$

e converrà procedere secondo Gordan(*) nel modo seguente. Essendo $y_0\, y_1\, y_2\, y_3\, y_4$ cinque quantità legate dalla (26), potremo porre

$$(27) \quad y_r = \varepsilon^{4r}\lambda_1\mu_1 - \varepsilon^{3r}\lambda_2\mu_1 + \varepsilon^{2r}\lambda_1\mu_2 + \varepsilon^{r}\lambda_2\mu_2$$

con che appunto, qualunque siano λ_1, λ_2 ; μ_1, μ_2 le (26) saranno verificate. È poichè inversamente segue dalle (27):

$$5\lambda_1\mu_1 = \sum \varepsilon^r y_r\,,\quad 5\lambda_2\mu_1 = -\sum \varepsilon^{2r} y_r\,,\quad 5\lambda_1\mu_2 = \sum \varepsilon^{3r} y_r\,,\quad 5\lambda_2\mu_2 = \sum \varepsilon^{4r} y_r$$

vediamo che comunque siano le y_r soddisfacienti alle (26), potremo dare a $\lambda_1\, \lambda_2$; $\mu_1\, \mu_2$ convenienti valori perchè le (27)

(*) V. Klein - Ikosaeder pag. 195.

siano verificate.

Poniamo per brevità

$$p_1 = \Sigma\, \varepsilon^{r} y_r\,, \quad p_2 = \Sigma\, \varepsilon^{2r} y_r$$

e indichiamo con p_1' p_2' ciò che diventano p_1 p_2 effettuando la sostituzione $(y_1\, y_2)\,,\,(y_3\, y_4)$, cioè:

$$\begin{cases} p_1' = y_0 + \varepsilon^2 y_1 + \varepsilon y_2 + \varepsilon^4 y_3 + \varepsilon^3 y_4 \\ p_2' = y_0 + \varepsilon^4 y_1 + \varepsilon^2 y_2 + \varepsilon^3 y_3 + \varepsilon\, y_4 . \end{cases}$$

La formola da verificarsi

$$\lambda' = \frac{(\varepsilon^4-\varepsilon)\lambda + (\varepsilon^2-\varepsilon^3)}{(\varepsilon^2-\varepsilon^3)\lambda - (\varepsilon^4-\varepsilon)}$$

diventa così:

$$(28)\quad (\varepsilon-\varepsilon^4)\, p_1\, p_2' + (\varepsilon^2-\varepsilon^3)\, p_2\, p_2' - (\varepsilon^2-\varepsilon^3)\, p_1\, p_1' + (\varepsilon-\varepsilon^4)\, p_2\, p_1' = 0 .$$

ora esprimendo $p_1\,,\,p_2\,,\,p_1'\,,\,p_2'$ per $\lambda_1\,,\,\lambda_2\,,\,\mu_1\,,\mu_2$ abbiamo

$$p_1 = 5\,\lambda_1\,\mu_2 \qquad p_2 = -5\,\lambda_2\,\mu_1$$

$$p_1' = \left\{2(\varepsilon^2-\varepsilon^3)+1\right\}\lambda_2\mu_2 + (\varepsilon+\varepsilon^4+3)\,\lambda_1\,\mu_2 - (\varepsilon^2+\varepsilon^3+3)\,\lambda_2\,\mu_1 + \left\{2(\varepsilon+\varepsilon^4)+1\right\}\lambda_1\mu_1$$

$$p_2' = (\varepsilon+\varepsilon^4+3)\,\lambda_2\,\mu_2 + \left\{2(\varepsilon+\varepsilon^4)+1\right\}\lambda_1\,\mu_2 - \left\{2(\varepsilon^2+\varepsilon^3)+1\right\}\lambda_2\,\mu_1 + (\varepsilon^2+\varepsilon^3+3)\,\lambda_1\mu_1$$

e sostituendo nella (28) troviamo in effetto che essa è identicamente soddisfatta.

Risulta di qui che se nella funzione razionale λ, data dalla (25), delle radici della proposta (23) eseguiamo le 60 sostituzioni del gruppo alterno sulle y_r, la funzione λ subirà precisamente le 60 sostituzioni lineari del gruppo icosaedrale. Se costruiamo quindi l'equazione icosaedrale (§.111)

$$(29) \qquad \frac{(\lambda^{20} - 228\lambda^{15} + 494\lambda^{10} + 228\lambda^5 + 1)^3}{12^3\lambda^5(\lambda^{10} + 11\lambda^5 - 1)^5} = Z$$

o più brevemente

$$(29^*) \qquad \frac{H^3(\lambda)}{12^3 f^5(\lambda)} = Z,$$

le cui radici sono i 60 valori di λ:

$$\lambda_1, \lambda_2 \ldots\ldots\ldots \lambda_{60}$$

il secondo membro $Z = \frac{H^3(\lambda_1)}{12^3 f^5(\lambda_1)}$, come funzione simmetrica di questi 60 valori, sarà una funzione semisimmetrica di $y_0\ y_1\ y_2\ y_3\ y_4$ e però razionalmente esprimibile per α, β, γ e $\sqrt{\nabla}$. La (29) o (29*) è quindi, come si voleva, una risolvente (di Galois) icosaedrale della proposta (23). Per il calcolo effettivo diretto di Z in funzione razionale di $\alpha, \beta, \gamma, \sqrt{\nabla}$ rimandiamo al libro di Klein (pag. 194 s. s.).

§. 119. — Formole per la risoluzione della equazione di 5° grado. Le considerazioni del §. precedente ci hanno dimostrata la possibilità di costruire una risolvente icosaedrale della equazione principale di 5° grado ciò che prova il teorema già enunciato al §. 117: L'equazione generale di 5° grado si può risolvere coll'aggiunta di una irrazionalità icosaedrica e con estrazioni di radici quadrate.

Resulta di qui che la risolvente principale di 5° grado (21) §. 115 della equazione icosaedrica deve potersi identificare con una equazione principale qualsiasi di 5° grado (23), disponendo convenientemente delle costanti m, n, z, le quali debbono potersi esprimere razionalmente per α, β, γ e $\sqrt{\nabla}$. Addiamo a constatare direttamente questo fatto e così avremo anche stabilite le formole di risoluzione per l'equazione generale di 5° grado mediante l'irrazionalità icosaedrica (*)

Identificando la (21) colla (23), abbiamo per determinare z, m, n le tre equazioni

$$(30)\quad \begin{cases} \frac{z\alpha}{3} = 8m^3 + 12m^2 n + \frac{6mn^2 + n^3}{1-z} \\ \frac{z\beta}{3} = -4m^4 + \frac{6m^2 n^2 + 4mn^3}{1-z} + \frac{3n^4}{4(1-z)^2} \\ \frac{z\gamma}{3} = 48m^5 - \frac{40m^3 n^2}{1-z} + \frac{15mn^4 + 4n^5}{(1-z)^2}, \end{cases}$$

dalle quali deduciamo, con semplice calcolo, le tre seguenti

$$(31)\quad \frac{12\beta m + \gamma}{12\alpha} = \frac{n^2}{1-z}$$

$$(32)\quad m\gamma - \frac{n^2\beta}{1-z} = \frac{9}{4z}\left(4m^2 - \frac{n^2}{1-z}\right)^3$$

$$(33)\quad \alpha^2 - \frac{4}{81}\frac{1-z}{n^2}(3m\alpha + 2\beta)^2 = \frac{1}{2}\left(4m^2 - \frac{n^2}{1-z}\right)^3$$

(*) Klein – l. c. pag. 192 e s.

Dal confronto delle ultime due deduciamo

$$\alpha^2 - \frac{4}{81}\frac{1-\xi}{n^2}(3m\alpha+2\beta)^2 = \frac{4}{9}\left(my - \frac{n^2\beta}{1-\xi}\right)$$

e sostituendo in questa per $\frac{n^2}{1-\xi}$ il valore dato dalla (31), otteniamo per determinare m l'equazione di 2° grado:

$$16(\alpha^4 - \beta^3 + \alpha\beta\gamma)m^2 - \frac{4}{3}(11\alpha^3\beta + 2\beta^2\gamma - \alpha\gamma^2)m + \frac{1}{9}(64\alpha^2\beta^2 - 27\alpha^3\gamma - 18\gamma^2) = 0$$

La risoluzione di questa equazione ci dà per m il valore

$$(34)\qquad m = \frac{(11\alpha^3\beta + 2\beta^2\gamma - \alpha\gamma^2) \pm \alpha\sqrt{\nabla}}{24(\alpha^4 - \beta^3 + \alpha\beta\gamma)},$$

avendo posto

$$(35)\qquad \nabla = 108\alpha^5\gamma - 135\alpha^4\beta^2 + 90\alpha^2\beta\gamma^2 - 320\alpha\beta^3\gamma + 256\beta^5 + \gamma^4.$$

Questo valore di ∇ è appunto il discriminante della equazione (23) (*)

Calcolato il valore di m dalla (34), scegliendo ad arbitrio l'uno o l'altro dei valori pel radicale $\sqrt{\nabla}$, potremo poi dedurne razionalmente ξ, ed alle osservazioni seguenti. Sostituendo nella (32) per $\frac{n^2}{1-\xi}$ il valore dato dalla (31) otteniamo infatti

$$(36)\qquad \xi = \frac{(48\alpha m^2 - 12\beta m - \gamma)^3}{64\alpha^2\{12(\alpha\gamma - \beta^2)m - 3\beta\gamma\}}$$

Per calcolare anche n scriviamo la prima delle (30) così:

$$\left(12m^2 + \frac{n^2}{1-\xi}\right)n = \alpha\xi - 8m^3 - 6m\frac{n^2}{1-\xi}$$

e ponendovi per $\frac{n^2}{1-\xi}$ il valore (31), troviamo la formola finale

---

(*) Si ha precisamente $\Pi(y_2 - y_3)^2 = 3125\,\nabla$

$$(37) \qquad n = \frac{12\alpha^2 Z - 96\alpha m^3 - 72\beta m^2 - 6\gamma m}{144\alpha m^2 + 12\beta m + \gamma}.$$

§. 120. — **L'irrazionalità icosaedrica come funzione modulare.** Terminiamo col dare un rapido cenno della risoluzione trascendente della equazione dell'icosaedro per funzioni ellittiche modulari, nella qual cosa dovremo naturalmente limitarci agli enunciati soltanto. Nella equazione dell'icosaedro

$$\frac{H^3(x)}{12^3 f^5(x)} = Z,$$

pongasi il parametro $Z = \mathcal{J}(\tau)$, essendo $\mathcal{J}(\tau)$ l'**invariante assoluto** dell'argomento τ (rapporto dei periodi) nella teoria delle funzioni ellittiche. La funzione algebrica x di $\mathcal{J}(\tau)$, resulterà allora, come $\mathcal{J}(\tau)$, una funzione **monodroma** di τ. $\qquad x = \xi(\tau)$

Ciò segue secondo il teorema di diramazione di Klein, dall'osservare che i punti di diramazione di x come funzione algebrica di $\mathcal{J}$ sono soltanto i tre $\mathcal{J}=0$, $\mathcal{J}=1$, $\mathcal{J}=\infty$ e attorno a $\mathcal{J}=0$ i 60 rami di x si permutano 3 a 3, attorno a $\mathcal{J}=1$ a 2 a 2. Il significato di $\xi(\tau)$ è allora perfettamente fissato se per un valore τ_0 di τ, tale che $\mathcal{J}(\tau_0)$ non sia $=0$, nè $=1$, nè $=\infty$, fra i 60 valori possibili per x se ne sceglie uno ad or-

tetrico.

La funzione tetrica modulare $J(\tau)$ rimane invariata solo quando l'argomento τ subisce una sostituzione $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$ del gruppo modulare Γ cioè una sostituzione lineare

$$\frac{\alpha\tau + \beta}{\gamma\tau + \delta}$$

con coefficienti interi e determinante $\alpha\delta - \beta\gamma = 1$. La funzione $\psi(\tau)$ per tutte queste infinite sostituzioni assume solo 60 valori distinti legati fra loro dalle sostituzioni del gruppo icosaedrale; le sostituzioni $\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix}$ che lasciano $\psi(\tau)$ invariata sono tutte e sole quelle in cui

$$\alpha \equiv \delta \equiv 1 \,, \quad \beta \equiv \gamma \equiv 0 \pmod 5$$

• come si usa scrivere:

$$\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix} \equiv \begin{pmatrix} 1, 0 \\ 0, 1 \end{pmatrix} \pmod 5 \,.^{(*)}$$

(*) Ciò risulta facilmente dall'osservare che le due sostituzioni elementari

$$A = \begin{pmatrix} 1, 1 \\ 0, 1 \end{pmatrix} \qquad B = \begin{pmatrix} 0, 1 \\ -1, 0 \end{pmatrix}$$

del gruppo Γ producono rispettivamente sopra ψ una sostituzione (icosaedrale) S a periodo 5 e una sostituzione T a periodo 2, laddove la sostituzione A, B a periodo 3 produce su $\psi(\tau)$ una sostituzione lineare a periodo 3. Se si applica

Questo gruppo, infinito come Γ, è un sottogruppo invariante di Γ d'indice finito = 60; esso è il sottogruppo relativo alla funzione modulare $\psi(\tau)$.
Il gruppo infinito modulare Γ è così posto in corrispondenza d'isomorfismo col gruppo finito icosaedrale G_{60}; ma il grado di moriedria è qui naturalmente infinito.

§. 121. — **Risoluzione trascendente dell'equazione dell'icosaedro.** Diamo da ultimo l'espressione analitica della trascendente icosaedrale $\psi(\tau)$. Si costruisca per ciò la trascendente $\sigma(u)\, w, w')$ di Weierstrass coi periodi

$$2w, \; 2w'$$

il cui rapporto $\frac{w'}{w}$ sia assunto $= \tau$. Indicando con $2\eta, 2\eta'$ i periodi di 2ª specie si ha per $\psi(\tau)$ l'espressione seguente:

---

allora il teorema di Dyck (Klein - Fricke frag..... e si osserva che A^5, B^2, $(AB)^3$ appartengono al sottogruppo $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \equiv \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix} \pmod 5$ ne segue assunto che ogni sostituzione $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ che lasci $\psi(\tau)$ invariata appartiene al detto sottogruppo e viceversamente.

$$(B)\quad \psi(\tau) = e^{(6\eta+8\eta')\frac{\omega}{5}}\ \frac{\sigma\left(\frac{2w}{5}\right)\sigma\left(\frac{2w+2w'}{5}\right)\sigma\left(\frac{2w+4w'}{5}\right)\sigma\left(\frac{2w+6w'}{5}\right)\sigma\left(\frac{2w+8w'}{5}\right)}{\sigma\left(\frac{4w}{5}\right)\sigma\left(\frac{4w+2w'}{5}\right)\sigma\left(\frac{4w+4w'}{5}\right)\sigma\left(\frac{4w+6w'}{5}\right)\sigma\left(\frac{4w+8w'}{5}\right)}.$$

Per le proprietà fondamentali della funzione σ si vede subito che la espressione del 2° membro dipende solo dal rapporto τ dei periodi ed è una funzione finita continua e monodroma di τ in tutto il semipiano positivo (τ asse reale escluso). Inoltre essa rimane invariata per tutte le sostituzioni $\frac{\alpha\tau+\beta}{\gamma\tau+\delta}$ del gruppo modulare che siano $\equiv \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \pmod 5$ (*). L'effetto delle due sostituzioni elementari $\tau+1$, $-\frac{1}{\tau}$ del gruppo modulare sopra $\psi(\tau)$ è dato dalle formole

$$(C)\quad \begin{cases} \psi(\tau+1) = \varepsilon^4\,\psi(\tau) \\ \psi\left(-\frac{1}{\tau}\right) = \dfrac{(\varepsilon^4-\varepsilon)\psi(\tau)+(\varepsilon^2-\varepsilon^3)}{(\varepsilon^2-\varepsilon^3)\psi(\tau)-(\varepsilon^4-\varepsilon)} \end{cases}$$

le quali danno rispettivamente sopra $\psi(\tau)$ le due sostituzioni elementari del gruppo icosaedrale. Introducendo la quantità

(*) Per verificarlo basta ricordare le formole fondamentali

$$\sigma(u\,|\,\alpha w+\beta w',\ \gamma w+\delta w') = \sigma(u\,|\,w\ w')$$

$$\sigma(u+2m\,w+2n\,w') = (-1)^{mn+m+n}\,e^{(2m\eta+2n\eta')(u+m\,w+n\,w')}$$

e rammentare inoltre che i periodi di 2ª specie η, η' subiscono la medesima sostituzione lineare di w, w'. Così pure si verificherà immediatamente la prima delle seguenti formole (C); quanto alla dimostrazione della seconda, essa è alquanto più riposta.

q di Jacobi $\qquad q = e^{\pi i \tau}$

e servendosi degli sviluppi dati dalla teoria delle funzioni ellittiche si trova per $\zeta(\tau)$ l'espressione analitica

$$(D) \qquad \zeta(\tau) = q^{\frac{2}{5}} \frac{\sum_{n=-\infty}^{n=\infty} (-1)^n q^{5n^2+3n}}{\sum_{n=-\infty}^{n=\infty} (-1)^n q^{5n^2+n}}.$$

Queste formole ci danno la risoluzione trascendente dell'equazione dell'icosaedro (e quindi dell'equazione generale di 5° grado) per funzioni ellittiche modulari nello stesso senso come la risoluzione di un'equazione di 3° grado può ottenersi per funzioni circolari. Dal valore assegnato di $Z = J(\tau)$ deduciamo per ciò un corrispondente valore di τ e colle formole precedenti troviamo $\zeta(\tau)$.—

FINE DELLA 2ª PARTE

Errata Corrige

			Invece di	leggi
pag. 25	riga	15	$=(x\ x_2 x_3 x_4 \dots\dots)$	$=(x_1 x_3 x_2 x_4 \dots\dots)$
„ 60	„	22	al quarto sono	al quarto non sono
„ 106	„	22		= go a $\frac{1}{2}$ sostituzioni.
„ 109	„	21		hanno per periodo $\frac{1}{2}$.
„ 124	„	3	iperboliche H di I	iperboliche si può com- porre un sottogruppo invariante H di I.—
„ 129			§. 41	§. 42
„ 144	formula	a)	$i\frac{\varepsilon^2 z+1}{z-1}$, $i\frac{\varepsilon z-1}{z+1}$	$i\frac{\varepsilon z+i}{z-i}$, $i\frac{\varepsilon z-i}{z+i}$
„ 151	riga	10	$\frac{a-bz}{az-b}=\frac{(\varepsilon^2a^2+\varepsilon^4b^2)z+(1-\varepsilon^2)ab}{(1-\varepsilon^2)abz+(\varepsilon^2b^2+a^2)}$	$=\frac{(\varepsilon^2a^2+\varepsilon^4b^2)z+(1-\varepsilon^2)ab}{(1-\varepsilon^2)abz+(\varepsilon^3b^2+a^2)}$
„ 152	„	5	$\varepsilon^2\frac{(\varepsilon^4-\varepsilon^3)\varepsilon^3z-(\varepsilon^4-\varepsilon)}{(\varepsilon^4-\varepsilon)\varepsilon^3z-(\varepsilon^2-\varepsilon^3)}$	$\varepsilon^2\frac{(\varepsilon^4-\varepsilon^3)\varepsilon^6z+(\varepsilon^2-\varepsilon^3)}{(\varepsilon^4-\varepsilon^3)\varepsilon^6z-(\varepsilon^4-\varepsilon\dots}$
„ 154	„	1		soppressa
„ 165	„	19	(ribaltamente) che.....	..... ribaltamente) attor- no agli assi che.....
„ 169	„	3	: 2°)	20 rotazioni a periodo 3 ete
„ 185	„	11	senso proprio	senso preciso
„ 186	„	20	intediamo	intendiamo
„ 188	„	10	sarebbe ridu cibile e cioè :	sarebbe riducibile. Da que- sto teorema seguono due corol- lari importanti e cioè :

pag. 197 riga 19 ~~tutti distinti~~ ~~non tutti~~ distinti

" 198 ultima formula $\mathfrak{F}(x_1 x_2 \dots x_n) = \mathfrak{F}_{s_1} = \Theta(V_{s_1})$

" 220 " 16 abbassava abbasserà

" 225 " 5 razionalità da cui razionalità in cui

" 232 " 10 z ε

" 255 " 5ª è risolubile ecc essa è risolubile ecc

" 258 " 9 scende scenda

" 264 " 14 il gruppo alterno al gruppo alterno

" 271 " 14 p^{δ} $p\delta$

" 296 " 13 l'ultimo termine dell'equazione di 2° grado in η si legge $\frac{1-(-1)^{\frac{p-1}{2}} \cdot p}{2}$

" 298 " 19 percorre z percorre con z

" 366 " 13 Nel primo termine della formola per p_1' invece di $\varepsilon^2 - \varepsilon^3$ leggi $\varepsilon^2 + \varepsilon^3$

Indice
della prima parte

§. 1.– Sostituzioni e loro composizione.	pag.	3.
2.– Periodo di una sostituzione.	"	6.
3.– Sostituzioni circolari.	"	9.
4.– Trasposizioni.	"	11.
5.– Sostituzioni simili – permutabili.	"	15.
6.– Gruppi di sostituzioni.	"	17.
7.– Teorema fondamentale.	"	19.
8.– Gruppo alterno.	"	23.
9.– Gruppi transitivi ed intransitivi	"	25.
10.– Teoremi sui gruppi transitivi.	"	29.
11.– Limite del grado di transitività	"	32.
12.– Gruppi imprimitivi e primitivi.	"	35.
13.– Teorema.	"	37.
14.– Gruppi isomorfi.	"	40.
15.– I gruppi generali di operazioni	"	43.
16.– Sottogruppi invarianti.	"	45.
17.– Gruppi semplici e composti.	"	49.
18.– Serie di composizione – Teorema di Jordan	"	53

§. 19.— Serie di composizione dei gruppi isomorfi. pag. 56.
20.— Sottogruppi invarianti del gruppo totale. " 58.
21.— Semplicità del gruppo alterno per $n>4$. " 60.
22.— Serie di composizione principale. " 64.
23.— Gruppi fattoriali e teorema di Holder. " 68.
24.— Gruppi complementari. " 70.
25.— Il primo teorema di Sylow " 72.
26.— Il secondo teorema di Sylow " 79.
27.— Dimostrazione. " 82.
28.— Gruppi di ordine p^2. " 85.
29.— Gruppi semplici degli ordini da 1 a 100. " 87.
30.— Gruppi semplici di ordine uguale a 60. " 91.
31.— Gruppi Abeliani " 92.
32.— Base di un gruppo Abeliano " 96.
33.— Invarianti di un gruppo Abeliano. " 99.
34.— Gruppi transitivi risolubili entro un numero primo di elementi. " 103.
35.— Gruppo metaciclico. " 106
36.— Rappresentazione analitica delle sostituzioni del gruppo metaciclico. " 109.
37.— Serie di composizione del gruppo metaciclico. " 111.
38.— Gruppo lineare totale entro p^n+1 indici " 113.

§. 39. – Periodo delle sostituzioni del gruppo lineare totale. pag. 118.
40. – Sostituzioni generatrici del gruppo modulare. " 121.
41. – Il gruppo modulare per $p > 3$ è semplice. " 125.
42. – Gruppi di sostituzioni lineari sopra una var.le " 129.
43. – Poli delle sostituzioni di un gruppo finito. " 132.
44. – Enumerazione dei possibili tipi. " 136.
45. – Gruppi ciclici e diedrali. " 138.
46. – Gruppo del tetraedro. " 142.
47. – Gruppo dell'ottaedro. " 145.
48. – Gruppo dell'icosaedro. " 147.
49. – La sfera complessa. " 152.
50. – Formola di Cayley. " 156.
51. – Movimenti di 2ª specie. " 160.
52. – Gruppi di rotazioni. " 163.
53. – Gruppi di rotazioni del tetraedro e dell'ottaedro. " 166.
54. – Gruppo dell'icosaedro. " 168.
55. – Orientazione dei poliedri regolari corrispondente alla forma normale dei gruppi. " 172.
56. – Gruppi ampliati. " 175.

Indice
della seconda parte

§. 57_ Irriducibilità. pag. 185

58 _ Irriducibilità nel campo assoluto di razionalità. " 188

59._ Risolvente di Galois. " 194

60._ Proprietà della risolvente di Galois. " 197

61._ Gruppo di Galois per l'equazione. " 202

62._ Proprietà caratteristiche del gruppo di Galois. " 205

63._ Riduzione del gruppo di Galois per aggiunta di quantità. " 208

64._ Transitività ed intransitività del gruppo di Galois. " 211

65._ Equazioni che hanno per gruppi di Galois il gruppo totale. " 212

66._ Formazione generale delle risolventi. " 216

67._ Gruppo della risolvente. " 218

68._ Equazioni del gruppo imprimitivo. " 221

69._ Riduzione di un'equazione composta a successive equazioni semplici. " 223

70._ Equazioni Abeliane " 226

§ 71.– Risoluzioni per radicali di un'equazione Abeliana a gruppo ciclico. pag. 230
72.– Modificazione della formola (A) di risoluzione. " 233
73.– Caso delle equazioni Abeliane a coefficienti reali. " 237
74.– Equazioni alle radici primitive p^{ma} della unità. " 240
75.– Riduzione nel gruppo di un'equazione per l'aggiunta delle radici di un'equazione ausiliaria. " 242
76.– Condizioni di risolubilità per radicali. " 247
77.– Irriducibilità per radicali delle equazioni generali di grado $n > 4$. " 251
78.– Risolubilità frazionale per radicali. " 254
79.– Aggiunta di una radice di un'equazione ausiliaria di grado primo. " 257
80.– Caso irriducibile della equazione cubica. " 261
81.– Risolventi di grado $< n$ della equazione generale di grado n " 263
82.– Risolvente di grado n della equazione di grado n. " 266
83.– Equazioni di grado primo risolubili " 271
84.– Risolvente di Lagrange " 274
85.– Il problema della divisione del circolo in n parti uguali " 275
86.– Irriducibilità dell'equazione " 278

87.- I periodi di Gauss pag. 281
88.- La risolvente $F_e(\eta)=0$. " 285
89.- Risolventi successive " 287
90.- Poligoni regolari inscrivibili nel cerchio colla riga e col compasso. " 290
91.- Inscrizione dei poligoni regolari di 5 e 17 lati. " 291
92.- La risolvente di 2° grado della equazione $\frac{x^p-1}{x-1}=0$. " 295
93.- Teorema di reciprocità nella teoria dei residui quadratici. " 298
94.- Applicazione delle formole di risoluzione delle equazioni Abeliane alle equazioni per la divisione del cerchio. " 300
95.- Formole fondamentali per le espressioni (ω^b, ε). " 301
96.- Formole di risoluzione per l'equazione $F_e(x)=0$. " 304
97.- I numeri complessi $\psi_n(d)$. " 307
98.- Decomponibilità dei numeri primi $p \equiv 1 \pmod e$ nel campo $(1,d)$. " 310
99.- Equazioni con un parametro. " 311
100.- Gruppo di monodromia e sue proprietà. " 314
101.- Il gruppo di monodromia come sottogruppo invariante del gruppo algebrico. " 316
102.- Funzioni algebriche e funzioni critiche. " 319

§. 103.– Nuova definizione del gruppo di monodromia. pag 323
104.– Punti di diramazione e sostituzioni elementari del gruppo di monodromia. " 326
105.– Funzioni algebriche i cui rami sono funzioni lineari l'uno dell'altro. " 327
106.– Costruzione delle equazioni dei poliedri regolari. " 330
107.– Gruppo di monodromia delle equazioni dei poliedri regolari. " 332
108.– Sostituzioni omogenee del gruppo icosaedrale. " 334
109.– Forme invarianti del gruppo omogeneo icosaedrale. " 338
110.– Costruzione delle forme icosaedrali f, H, T. " 342
111.– L'equazione dell'icosaedro " 344
112.– Metodo invariativo di Klein per la formazione delle risolventi. " 346
113.– Le forme ottoedrali $\underline{t}$ e $\underline{W}$. " 349
114.– Le risolventi di 5° grado delle $\underline{u}$ e delle $\underline{v}$. " 352
115.– La risolvente principale delle Y. " 355.
116.– La risolvente di 6° grado " 358
117.– L'equazione generale principale di 5° grado e la sua risolvente di Galois icosaedrale. " 361
118.– La radice λ della risolvente icosaedrale " 364